EXHIBIT 7

CipherBlade

Blockchain Investigation Agency

EXPERT REPORT

Matter:	Williams v. AT&T Mobility LLC
Author:	Richard A. Sanders
Date:	August 2, 2021

I. INTRODUCTION

1. My name is Richard A. Sanders. I am a co-founder and lead investigator of CipherBlade, a blockchain forensics and cybercrime investigative firm which consults on some of the most renowned blockchain projects, as well as numerous law enforcement and regulatory investigations, and provides advisory services to cryptocurrency exchanges and other organizations. Prior to co-founding CipherBlade, I was in the United States Army, where I attained the rank of a Staff Sergeant and spent 12 years as a forward observer and PSYOP specialist. A copy of my C.V. is attached as Exhibit A.

2. I understand that Plaintiff Jason Williams is claiming in this action that he suffered damages allegedly resulting from seven (though AT&T's records reflect six) unauthorized SIM swaps on his AT&T wireless account from November 2018 to February 2019. Specifically, Mr. Williams claims that approximately 0.23 Bitcoin was stolen from him as a result of an unauthorized SIM swap on November 5, 2018, and that he was also forced to shut down his cryptocurrency mining operation in February 2019 due to an unauthorized SIM swap on February 6, 2019.[1] He further alleges various emotional damages.[2]

A. Scope of Assignment

3. I have been retained by AT&T Mobility LLC (AT&T) to provide expert services in the matter of Jason Williams v. AT&T Mobility LLC, No. 4:19-cv-00153. I was asked to provide an overview of cryptocurrency, and the associated risks and responsibilities of holding or mining cryptocurrency. I was also asked to provide my expert opinion with respect to the alleged breaches of Mr. Williams' third-party accounts, how criminal SIM swappers attempt to breach third-party accounts, Mr. Williams' personal online conduct and cybersecurity practices, whether or how the

[1] Complaint ¶¶ 42, 76-77.

[2] Complaint ¶ 178.

unauthorized SIM swaps or Mr. Williams' actions may have played a role in Mr. Williams' alleged damages, and how those alleged damages could have been prevented. I am being compensated at my standard rate of $775 per hour for my work on this matter. My compensation is not dependent upon my analysis or conclusions as contained in this report.

4. In performing the analysis and reaching the conclusions set forth herein, I considered the documents and materials contained in the Exhibits to this report, the pleadings and discovery materials in this case, as well as my independent research regarding Mr. Williams' online activity and additional publicly available information about unauthorized SIM swaps and cryptocurrency losses. This included reviewing Mr. Williams' social media accounts, media and articles concerning or quoting Mr. Williams or these incidents, as well as querying Mr. Williams through public databases including DeHashed and TruthFinder.

B. Qualifications

5. I have experience in some of the most well-known cryptocurrency investigations, including hacks of prominent individuals (high net-worth individuals ("HNWIs") and/or influencers), companies, and exchanges. As one example, I served as a core investigator, gathering evidence which led to the identification, arrest, and prosecution of a notorious theft ring that conducted immense SIM-swapping. The takedown of the aforementioned ring is one example in a long resume of accomplishments for the CipherBlade team. There are few experts in the field with expertise in all of the subjects that my investigations often cover, which include blockchain forensics, cryptocurrency AML, and cryptocurrency cybercrime investigation. My team, including me personally, has experience in hundreds of cryptocurrency cases.

6. In addition to my duties with CipherBlade, I serve as a volunteer with Crypto Defenders Alliance[3] (CDA) — an organization with representatives from nearly all major cryptocurrency exchanges and services, with the purpose of combating laundering of illicitly obtained funds. I was selected as one of the CDA's four administrators due to my demonstrated expertise as a blockchain forensics expert, and my cybercrime investigation knowledge, and leadership. CDA has been a core component in the prevention of laundering of illicitly-obtained funds from many significant cryptocurrency hack and scam situations, as well as numerous major cryptocurrency exchange hacks. My duties within CDA, as well as my duties within CipherBlade, entail on a daily basis determining terminal destinations of stolen cryptocurrency and consulting with legal and law enforcement professionals on the investigative and recovery process.

7. I also serve as a volunteer with the Anti-Human Trafficking Intelligence Initiative (ATII) where I provide critically needed blockchain analysis and other insight in some of the most severe crime typologies. Specifically, I provide actionable analysis, intelligence, and advisory to takedown purchasers and distributors of child sexual abuse material. As just one example, in November of 2020 alone, in partnership with law enforcement, I executed a "dusting"[4] raid on 46 different Bitcoin wallet addresses connected to child sexual abuse material, resulting in the identification of clusters of Bitcoin wallet addresses that assisted or will assist law enforcement efforts to identify potentially hundreds of purchasers of such material and potentially the means by which distributors of such material "cash out." Law enforcement, in this case the Department of Homeland Security through the Immigration and Customs Enforcement, has routinely sought my advice and

---

[3] https://cryptodefendersalliance.com/

[4] A "dusting" raid raid involves sending tiny amounts of cryptocurrency to certain wallets and subsequently tracking the transactional activity of the wallets to ascertain the identity of the person or entity who controls the wallet at issue. See https://academy.binance.com/en/articles/what-is-a-dusting-attack.

consultation on relevant topics such as Bitcoin mixers throughout this process. This work is strictly on a volunteer basis.

8. My professional relationship with government officials is not limited to law enforcement, but includes extensive interfacing with regulatory agencies as well. I am routinely contacted by regulatory agencies both within and outside of the US for insight on the industry, potential regulations, insight on pressing issues, best practices, and even assistance in cases relating to cryptocurrency and cybersecurity issues. While particular agencies and cases are subject to nondisclosure, I have been personally retained by government agencies both in and outside of the US for expert services in related matters.

9. My core expertise, however, is blockchain analysis, also known as blockchain forensics. While blockchain analysis is a relatively new and evolving field that, because of its nascency, has limited options for formal training and certification, there is often a need for this type of analysis in an array of cryptocurrency investigations and/or legal disputes. In order to perform blockchain analysis, I will often utilize a tool such as Chainalysis Reactor, CipherTrace, Crystal, or Elliptic. At a basic level, these tools enable one to "visualize the blockchain" by taking publicly-available information such as wallet addresses and blockchain transactions that would otherwise be contained in spreadsheets, and visualize them, typically in graphs. For instance, just like a traditional investigator can visualize various connections between suspects and other individuals using a corkboard and strings of yarn, a blockchain analyst can use software to visualize a complex web of transactions involving multiple cryptocurrency wallets. There are numerous sophisticated parts of blockchain analysis that require insight and experience in order to perform the work effectively, but in simplified terms, these type of tools enable analysts and investigators to "follow the money." It is also critical to note that each of these tools has varying degrees of efficacy, largely due to

attribution (labeling of wallet addresses), which is why Chainalysis is considered to be industry standard and is the tool my firm utilizes primarily.

10. As mentioned in the preceding Paragraph, there are very few training programs in existence to become a blockchain analyst/cryptocurrency crime investigator. Given the dearth of such training programs, Chainalysis launched its Certified Investigative Partner (CIP) program to increase the pool of available experts on issues concerning cryptocurrency and blockchain related cybercrime. CipherBlade was a premier CIP upon the reveal of this program, and I was personally quoted in the announcement. Chainalysis, as well as other blockchain forensics tool providers, frequently refer work concerning blockchain analysis/cryptocurrency crimes to CipherBlade.

11. As a Co-Founder of a firm primarily known for assisting victims of cryptocurrency theft and having had handled hundreds of such cases, I have an extensive understanding of the means and methods employed by criminals operating in the cryptocurrency sphere across the entire spectrum: anything from a SIM-swapper stealing funds from inexperienced or reckless cryptocurrency holders who disregard security warnings or fail to implement appropriate security practices, to a more "white collar" criminal who cons investors in violation of financial regulations.

12. Whether it is in the context of a thief that stole cryptocurrency from an individual with inadequate security, an ex-husband hiding cryptocurrency in a divorce proceeding, or an Initial Coin Offering ("ICO") executive embezzling funds, I have substantial experience in investigating matters involving digital assets, uncovering the truth, and reducing my findings to understandable language.

13. As a result of my involvement in hundreds of cybercrime investigations, I have a deep understanding of cybercriminals' methods from the standpoint of both passive observation (from analysis of post-mortem casework) and active analysis, such as investigating active groups, sometimes in an undercover capacity, or simulating cybersecurity attacks to expose vulnerabilities

in a client's existing security practices. This understanding of how cybercriminals conduct their attacks is of immense value in preventing or mitigating further attacks, and my ability to "stand in the shoes" of such criminals is why I am often requested to speak on panels and with the press about these matters.

14. Consequently, I also have a detailed, experiential understanding of the ways consumers leave themselves needlessly vulnerable to cyberattacks, the majority (if not all) of which could be easily prevented via appropriate cyber hygiene, implementing basic cybersecurity practices, or simply following instructions. Oftentimes, the particular vulnerability that is exploited as part of a cyberattack is the result of an individual's decision to simply ignore warnings or refuse to follow instructions regarding security practices that are solely within their control and ability to implement.

15. Because of my experience, I have been asked to appear on a multitude of podcasts, speaking engagements, and press interviews on a wide range of security- and cryptocurrency-related topics, including the topics of unauthorized SIM-swaps[5] and the basic security measures that any cryptocurrency holder should employ to prevent any resulting loss.[6] My expertise has been requested by influencers seeking to educate the public in cryptocurrency fraud prevention.[7] I consult on questions throughout the field, including such core issues as "how do I avoid getting hacked," or "how do I avoid getting scammed."

C. Summary of Opinions

16. Below is a summary of my expert opinions. While this list is not exhaustive, it covers the key points and supporting analysis that are described more extensively through this report.

---

[5] https://www.sho.com/vice/season/1/episode/1/keepers-of-the-caliphate-and-sim-kids

[6] https://unchainedpodcast.com/how-to-keep-your-crypto-from-being-stolen-via-your-phone/

[7] https://youtu.be/0HHZnFBTESw

- Mr. Williams employed inadequate and reckless personal security and cyber hygiene practices, far below the standards of what any responsible participant in the cryptocurrency industry should utilize. Far more than anything he alleges, AT&T did or failed to do, it was Mr. Williams' own actions (and inactions) that enabled criminal hackers to successfully and repeatedly target him, and exploit the inadequate security he employed on the accounts he maintained with third parties like Google, Slush Pool, and Coinbase.
- Mr. Williams' conduct evinces a lack of personal accountability for his own actions that enabled the breaches of his third-party accounts. Mr. Williams seeks to blame AT&T for the consequences of hackers accessing those accounts, despite the facts that AT&T has no information about those accounts nor any ability to control how those accounts are secured, and it was Mr. Williams who had the sole ability to properly secure his private accounts and could have done so through mere minutes of effort.
- A SIM swap itself does not provide the bad actor with access to Mr. Williams' third-party accounts. Rather, there are intervening steps that must occur before a hacker could access such accounts. As of the date of this report, Mr. Williams' document productions (JW_0001-75) and discovery responses, as well as the materials produced by third parties such as Coinbase and Gemini, do not establish that the SIM swaps, rather than some other intervening event(s) — including but not limited to Mr. Williams' own negligence and/or repeated failures to employ reasonable personal security measures — caused the breaches of his third-party accounts or the harms he alleges in the complaint.
- With reference to the intervening steps that must occur between a SIM swap and the ultimate breach of Mr. Williams' third-party account(s), there are numerous simple security actions Mr. Williams could have and should have taken that would have prevented the hackers from accomplishing each of those steps. Taking such actions would have prevented

the harms Mr. Williams alleges, regardless of whether an unauthorized SIM swap occurred on his AT&T account.

- Regarding the alleged diversion of BTC from Mr. Williams' mining operation, the only way to substantiate that allegation is via records from Mr. Williams' Slush Pool account, which I understand have not been produced.

II. CRYPTOCURRENCY OVERVIEW

17. Cryptocurrencies are digital representations of value which rely on blockchain technology — a distributed ledger of all transactions that is decentralized and unable to be changed under most circumstances — to record transactions. The most well-known form of cryptocurrency is Bitcoin, the first cryptocurrency ever developed, which has boasted the broadest adoption and highest market capitalization of all cryptocurrencies ever since.

18. While Bitcoin is largely regarded as the Godfather of cryptocurrency, the past several years has seen the proliferation of "altcoins" (cryptocurrencies other than Bitcoin), including Ethereum, which is second to Bitcoin in terms of market capitalization as of this writing. Today, there are numerous different types of cryptocurrency, numbering more than 2,000 by some counts.

A. Cryptocurrency Mechanics

19. Cryptocurrency is different from fiat money (i.e., government-issued currency like U.S. Dollars) in that cryptocurrency cannot be stored in any location or exist anywhere in a physical form. Rather, cryptocurrency ownership is reflected on a publicly viewable online ledger called the "blockchain," which is a continuously growing list of records reflecting all transactions for the particular type of cryptocurrency.

1. Private Keys

20. Any cryptocurrency asset (such as some amount of Bitcoin) is associated with a "public address" (or "public key") that is publicly known and essential for identification, and a non-public

"private key" that used to spend cryptocurrency. A public address is a location identified by a hash (e.g., 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX), and is roughly analogous to an email address or a bank account — a unique and secure identifier that allows for the transmission of cryptocurrency from one user to another. Each public address is associated with a unique private key (also a series of letters and numbers), which together form a public—private key pairing. While not critical to my opinions, it is worth noting that the public address associated with a given private key is itself derived from the private key using the specific requirements of the cryptographic algorithm associated with the particular type of cryptocurrency. In other words, the public address is essentially reverse-engineered from the applicable private key, although the private key cannot be determined from a public key or public address.

21. At a high-level, a private key can be thought of as a predetermined password that is required to spend cryptocurrency from the associated public address. If the private key is lost or forgotten, the associated cryptocurrency assets are lost forever, orphaned on the blockchain with no possibility of being spent ever again. On the other hand, the private key alone is sufficient to spend cryptocurrency from the associated public address. In this sense, the private key is what grants the cryptocurrency holder ownership of the assets in the corresponding public address. It is therefore paramount for a holder of cryptocurrency to keep their private keys secured, both to reduce the risk that private keys are lost or forgotten and to reduce the risk that private keys fall into the wrong hands. If either risk materializes, a cryptocurrency loss typically results.

2. Cryptocurrency Wallets

22. The ability to "be your own bank" through "self-custodial" cryptocurrency wallets is often referenced as a primary draw to cryptocurrency. Self-custody involves maintaining your own private keys to your own wallet, and is comparable to having a physical personal wallet: you have direct control over your funds and don't need to trust a third party, such as a bank or exchange, to

access your funds. Keeping cryptocurrency on a centralized service (such as an exchange), on the other hand, would be considered utilizing a "custodial service" and is more akin to having a bank or brokerage account because you have to go through that service to access your funds and trust that service to hold your funds and provide access to them when requested.

23. A cryptocurrency "wallet" is a mechanism that stores and/or generates public—private key pairs (often, via a "seed phrase," which is a series of words used to deterministically generate public—private key pairs), and enables its user to send and receive digital currency and monitor their balance. However, unlike traditional pocket wallets, cryptocurrency wallets do not actually store any currency. All that exists are records of transactions stored on the blockchain. Thus, when a person sends a cryptocurrency to another person, they are essentially signing off ownership of their currency to the receiver's wallet address. There is no actual exchange of physical coins; the transaction is signified by the transaction record on the blockchain and a change in balance in the owner's wallet in the public ledger. This is why blockchains are considered to be, and are often referred to as a form of distributed ledger technology.

24. There are three main varieties of cryptocurrency wallets—hardware wallets, software wallets, and paper wallets. All are essentially what they sound like—a separate hardware device, a software program, or a literal piece of paper, respectively.

- **Hardware wallets.** Keys are stored in a hardware device without an internet connection, and are utilized by connecting the device to a computer (whether through a physical connection, bluetooth, etc.); the private keys are stored in such a way that they can be utilized to transact but otherwise are not accessible. In essence, the keys are contained in the hardware wallet and not transferred elsewhere; the computer only receives the signed transaction, not the private key.

- **Software wallets.** Keys are stored electronically, typically in encrypted format, and can be accessed directly on a computer without needing an external mechanism like a hardware device or a QR code printed on a sheet of paper.
- **Paper wallets.** Stored keys are typically accessed from a paper wallet by scanning a QR code. Paper wallets were a concept pre-dating the invention of hardware wallets. While some still do use paper wallets, they are (and have been) reported to be a generally inferior option to hardware wallets.

25. Hardware and paper wallets are commonly referred to as "cold wallets" because they have no connection to the internet. Instead, they use a physical medium to store keys offline, making them resistant to attempts to gain unauthorized access. It is effectively impossible to compromise such wallets without physical access to the particular hardware device or piece of paper. On the other hand, software wallets (such as Electrum or Metamask), are "hot wallets" that are connected to the internet in one way or another, and do not require a separate external item. While this may afford marginally more convenience for wallet holders engaging in frequent transactions, hot wallets are, as a general matter, easier to compromise if not properly secured.

26. Almost all hardware and software wallets share a common factor in the setup process: seed phrases, which are generated upon wallet setup and are the backup in case a device (whether the hardware wallet, or the computer/phone for the software wallet) is replaced, lost, or destroyed. Specifically, a seed phrase works like a root key that generates and gives access to all keys and addresses in the associated wallet. Much like private keys, a compromise of a seed phrase means that the ability to send funds is enabled for bad actors.

27. The security warnings/setup instructions for nearly all cryptocurrency wallets emphasize the importance of keeping private keys and seed phrases secure. When a cryptocurrency user sets up a wallet, instructions specifically state to not store the seed phrase electronically, often

emphasizing this instruction with requirements that state "write this down," or even being provided a booklet to do exactly that.

28. Software wallets also typically offer additional Security Measures that may be activated on a user's account. For instance, the cryptocurrency wallet service Exodus offers the ability to implement a type of two-factor authentication ("2FA"). Additionally, wallet services typically offer the ability to implement a "passphrase" requirement, an additional security measure in the event of a seed phrase compromise so that a bad actor would need both the passphrase and the seed phrase to have the credentials necessary to spend the associated cryptocurrency assets, which prevents unauthorized access to a seed phrase from resulting in cryptocurrency theft.

29. Above all else, when it comes to self-custodial wallets, quite simply all the responsible participant needs to do in order to not lose their cryptocurrency to theft is to follow the instructions presented during setup of the wallet: Never store your private key or seed phrase electronically. If the cryptocurrency participant follows those instructions, it is impossible for a remote hacker to steal their cryptocurrency.

B. Cryptocurrency Risks

1. Cryptocurrency Transactions Are Irreversible.

30. Cryptocurrency transactions are irreversible and lack the type of safety net from centralized companies in the fiat money space, such as credit card chargebacks and the ability to reverse unauthorized bank transactions. Understanding the irreversible nature of cryptocurrency transactions and the associated implications presents a well-known and baseline requirement for individuals engaging in cryptocurrency dealings to properly secure their digital assets.

31. Precious metals offer an illustrative analogy as another type of asset for which a theft cannot be "reversed." Those who invest in precious metals either pay for someone to store their precious metals in vaults, or if they keep their precious metals themselves, properly secure them with varied

security measures, most commonly under lock and key. That key is presumed to be safely guarded by the holder (not stored under a doormat, or in a place that, for example, a landlord for a work order would stumble across) as the precious metals investor knows that if the key is compromised, the person that gained access to that key, consequently, can access their precious metals. The same approach, and in fact more importantly (since cryptocurrency can be instantly and irreversibly transferred to a wallet owned by anyone in the world), applies for digital assets.

2. Centralized Custodial Services, And Their Users' Wallets They Maintain, Can Be Compromised.

32. Despite a well-known catchphrase of the cryptocurrency space, "not your keys, not your coins,"[8] cryptocurrency users may also choose to entrust their keys (and their coins) to a centralized exchange or other service (such as Coinbase) that holds the assets in wallets under its control and executes orders on behalf of the account holder, as opposed to the users storing their keys in their own custody — in wallets they control and to which they have direct access. Effectively, what such centralized custody services provide is comparable to an "IOU" in faith that the service will be able to process a withdrawal for the amount displayed on the user's account if and when the withdrawal is demanded. This is roughly comparable to a bank account and a traditional wallet: I can say I own $100 in my wallet and show a particular $100 bill, whereas $100 in a bank account is an IOU. In either case, I am also responsible for securing the means of access of my wallet and my bank account.

33. However, by entrusting digital assets to a centralized custodial service, the account holder largely relinquishes control over the protection and security of those assets independent of the security features activated on their own account. Security threats to centralized custodial services may come from outside parties or from insiders who are associated with the service itself.

[8] https://www.ledger.com/academy/not-your-keys-not-your-coins-why-it-matters

Numerous instances of cryptocurrency exchange compromises and/or misappropriation of custodial assets in recent years that have resulted in billions of dollars' worth of financial loss for customers.

34. Despite such concerns regarding centralized cryptocurrency services, they still have their place in the ecosystem as on-ramps (places to deposit and withdraw fiat money) and to a lesser extent (due to the rise in decentralized exchanges, where users hold their own assets) to trade digital assets. However, many cryptocurrency users choose to keep cryptocurrency on centralized services, and common consensus[9] is that keeping *some* (but not *all* or even *most*) of your digital assets with centralized services, based upon risk appetite, is a sensible middle-ground. Much like the importance of protecting credentials such as private keys and seed phrases for self-custodial wallets, account holders for centralized services must protect their login credentials for the same reason: cryptocurrency transactions are irreversible.

3. Cryptocurrency Values Are Extremely Volatile.

35. Whether considered a virtue or a vice, the truth is that cryptocurrencies are and have always been *extremely* volatile assets. For example, after spiking during the bull market of 2017, the exchange rates of Bitcoin and Ethereum plummeted by around 80% through the bear market from 2018 continuing into 2019. Short-term swings can also be very extreme. For instance, as recently as May of this year, the exchange rate for Ethereum reached its all-time-high of over $4,300/ETH on May 12 and subsequently plunged to under $2,000/ETH at a low point on May 19, 2021, a decline of over 50%. Bitcoin similarly declined from around $60,000/BTC to $40,000/BTC over the same period. Indeed, the bulk of these price dips occurred within a mere 24-hours on May 19, stoking fears of the next "crypto winter" following a strong rally beginning in mid-2020.

---

[9] https://www.dowallet.app/blog/3-reasons-you-should-not-leave-all-your-crypto-on-an-exchange.html

4. Cryptocurrency Is an Attractive Target for Cybercrime.

36. Cryptocurrency is an increasingly prevalent target among cybercriminals seeking financial gain, due in large part due to the irreversible nature of cryptocurrency transactions, the relative lack of regulation, and that there are generally more and easier methods of "laundering" stolen assets to conceal their source or destination compared to fiat money.

37. The recent cryptocurrency "bull markets" in 2017 and more recently starting in late-2020 have ushered in a wave of new speculative investors of all varieties, individuals and entities alike. While some new participants are very knowledgeable regarding risks and appropriate security (as one example, due to prior experience with decentralized technology), many are not. Regardless of the baseline knowledge these new participants have, there are ample resources to begin or expand their knowledge base, which is needed to be a responsible participant in this space.

38. Anyone who is broadly known to hold, or even *suspected* of holding significant quantities of cryptocurrency, is a high-risk target for cybercriminals.[10] This includes a public figure or a well-known company in the cryptocurrency industry, or even high net-worth individuals more broadly. For such persons and entities, adequate cryptocurrency security practices become all the more important—at an absolute and bare minimum, following the instructions in their wallet/exchange setup, and spending a modest amount of time (and/or money) researching and implementing appropriate security practices.

39. Mr. Williams is a prime example of a high-risk target for cyberattacks and cryptocurrency theft, both as a founder and partner at Morgan Creek Digital, an investment firm focusing on digital

[10] Anyone (regardless of notoriety) who holds cryptocurrency is at risk for cyberattack for the same reason that, as a rule, anyone is at risk for cyberattack. For example, compromised passwords (common with data breaches) are routinely used in attacks called "credential stuffing," wherein email/password combinations are used to attempt logins to other accounts, including cryptocurrency exchanges or email accounts.

currencies and blockchain technologies,[11] and as a HNWI with a "significant social media presence" where he frequently discussed his cryptocurrency and his wealth[12] prior to the first alleged SIM swap incident in November 2018. With his background and activity, as well as his over 138,000 followers on Twitter, Mr. Williams is a public figure in the cryptocurrency industry, and by his own admission was therefore "at a heightened risk" for cyberattacks (like unauthorized SIM swaps) aimed at stealing his cryptocurrency. And given he currently occupies position #66 on Cointelegraph's "Top 100" notable people in the cryptocurrency industry,[13] not to mention the publicized[14] $500M sale of an urgent care company that he founded, Mr. Williams is a quintessential example of a high-risk target for cyberattacks and attempted cryptocurrency theft.

C. SIM Swaps and Cryptocurrency Theft

40. The only way a thief can steal cryptocurrency is if the thief obtains the credentials necessary to access the victim's wallet or account and then transfer or divert the cryptocurrency from that wallet or account. Thus, it is critical that cryptocurrency users follow security warnings and instructions when setting up their wallets and accounts. It is also critical, however, to properly secure email accounts (*e.g.*, Google/Yahoo) because users will often link their email accounts to other accounts they maintain, thus making the unauthorized access of the former a gateway to unauthorized access of the latter. Indeed, in this case, Mr. Williams revealed that access to his Google account would permit access to other accounts he alleges hackers breached.[15]

41. A SIM swap alone does not provide the perpetrator with access to anything beyond control of the target's phone number—not any accounts, not any communications, and certainly not any

---

11 Compliant filed Oct. 25, 2019 [Doc. 2] ("Compl.") ¶ 8.

12 Compl. ¶ 8; *see* Exhibit B at pp. 16, 21-24, 27-31.

13 https://cointelegraph.com/top-people-in-crypto-and-blockchain/jason-williams

14 *See, e.g.*, https://fiftyonepercent.podbean.com/e/jwiliams/

15 *See* Plaintiff's response to Interrogatory No. 2 (July 6, 2020).

cryptocurrency credentials or cryptocurrency itself. Moreover, confidential personal information about the target — and certainly the types of confidential information a phone company would have about one of its subscribers — is not needed by a criminal seeking to take over the target's private accounts or steal cryptocurrency because information about the account holder does not provide access to cryptocurrency credentials or cryptocurrency itself. Accordingly, it is not my experience that a criminal seeking to steal cryptocurrency (in a similar capacity) would need to obtain confidential information about the target himself/herself in order to access the target's accounts and wallets, because such information would not be required for accomplishing those objectives.

42. To the extent a SIM swapper is able to access any of the target's accounts, communications, or cryptocurrency, the swapper must have first proceeded through intermediate steps to — steps that the target can easily prevent by implementing basic security measures to protect his/her private accounts from being accessed by someone who has taken temporary control of his/her mobile phone number. Stated differently, following an unauthorized SIM swap, the perpetrator must then also successfully exploit defects in the target's own personal security practices (namely, security settings) before access to any of the target's online accounts is possible. Access to accounts is not possible only by means of a phone number unless that is a setting the individual put or left in place deliberately, such as by enabling a feature that allows an account's password to be reset with a code sent to that phone number. But even then, the perpetrator would still need to know what online accounts their target maintains (or where they store their cryptocurrency) and which email address and/or "user names" the target uses to access those accounts — information neither maintained by phone companies nor gained through a SIM swap.

43. For instance, in Mr. Williams' case, he contends the third-party criminals used their control of his phone number to reset the password to his Google account and gain access to that account,[16] an intermediate step that was easily preventable if Mr. Williams had chosen a security configuration that does not include SMS password reset. A phone number by itself cannot access an email account,[17] unless the owner of that email account elects to use that phone number as a means of reset[18] — and even in that case you would still need to know the email address or user name of the account. Access to a phone number does not provide access to an email app nor the credentials to an email account. Further, how one accesses an email account has no bearing on how that email account is secured. For example, I secure a Google account with Google Authenticator (as a means to log in), but I access it (read my emails once logged in) on my phone.

44. Nor does a phone number provide access to files or cryptocurrency. Files and data stored on a cell phone would not be directly accessible via a SIM swap. A clone of the phone's memory is not transferred via an unauthorized SIM swap, only temporary control of a phone number is. And while a text message to a phone number can be used to reset account passwords if an account holder *affirmatively chooses* to allow that, that scenario simply underscores how simple it is to insulate an account from being accessed following an unauthorized SIM swap: do not turn that option on — it is well-known among cryptocurrency users to be fragile.

45. For example, Google Authenticator 2FA is a well-known, free, and easy-to-use method for securing accounts through Time-Based One-Time Pins ("TOTP"), which requires access to a

---

[16] Plaintiff's Response to Interrogatory No. 2 (Jul. 6, 2020).

[17] Even SMS 2FA (as opposed to SMS password reset) would still require the person attempting access to know the account holder's password.

[18] SMS password reset is *not* SMS 2FA, and is a feature commonly exploited and used by SIM-swappers.

particular physical device to obtain 2FA access codes in order to log into accounts.[19] If an unauthorized third party takes control of a phone number through a SIM swap, he or she cannot access Google Authenticator 2FA codes because the phone number is not used to transmit those codes, and thus cannot access any accounts secured by Google Authenticator. Rather, to access an account that is properly secured by Google Authenticator, the criminal would need to literally steal the victim's physical phone (and know the code to unlock it) and open the Google Authenticator app to obtain the TOTP 2FA codes.

46. Phone companies do not have any knowledge of, or ability to control, the security measures its subscribers utilize on their private third party accounts, let alone their personal cryptocurrency wallets. At bottom, it is an individual's responsibility to secure their private accounts, especially against known cyberattack methods such as SMS password resets following an unauthorized SIM swap. While an unauthorized SIM swap grants the perpetrator a short window of time to send and receive calls and messages[20] using an individual's phone number (until the individual calls the phone company to have the SIM swap reversed), it is the actions and personal security choices of that individual which determine whether the perpetrator can access any of their third-party accounts.

47. In my experience, nearly every cryptocurrency theft I have investigated could have been prevented had the victim simply followed their wallet set-up instructions and security warnings and/or taken basic steps to secure their accounts such as by using Google Authenticator 2FA.

---

[19] "Time-based One-Time-Pins," or TOTP, is a form of two factor authentication that uses a code displayed by an application on your phone, and which continually resets to a new code after a set period of time (*e.g.*, every 20, 30, etc. seconds). The code can only be seen on the user's phone screen and thus, unlike a code sent via a text message, cannot be seen or intercepted by a SIM swapper. "Google Authenticator" and "Authy" are the most well-known and free TOTP mobile phone apps. *See* https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm.

[20] Standard phone SMS/MMS messages (commonly called "text messages"); note this does not apply to account-based messages such as WhatsApp, Signal, Telegram, etc. which are login-based and, much like login-based accounts, have varied security options.

III. THE RESPONSIBLE CRYPTOCURRENCY PARTICIPANT

48. As stated above, there has been an influx of new participants in the digital assets space in years past, especially following the late 2017 "bull market." These new participants range from being very knowledgeable about the risks of cryptocurrency and how to implement appropriate security measures, to having almost no knowledge of those subjects. Regardless of the baseline knowledge these new participants have, there are ample resources to begin or expand their knowledge base, which is needed to be a responsible participant in this space.

49. Responsible cryptocurrency participants do their research to understand and appreciate the unique risks of participating in the cryptocurrency industry, follow security instructions and implement appropriate personal cybersecurity practices, and practice good cyber hygiene.

A. Understanding the risks and implementing appropriate security measures.

50. Individuals who hold cryptocurrency are presumed to follow instructions, heed warnings, and leverage the industry catchphrase "DYOR" (do your own research). This includes reviewing publicly-available information on proper cybersecurity practice, such as utilizing password managers, TOTP or hardware-key 2FA, and not relying on a single point of failure such as a telephone number, or SMS password reset.[21]

51. The responsible cryptocurrency participant does this research and also reviews news and trends for the industry (as would investors in any other type of asset) to stay abreast of the commonly-discussed dangers presented with reusing passwords or relying on a single, centralized point of failure such as SMS 2FA.[22] Rather than presume "it can't happen to me," a responsible

[21] https://medium.com/mycrypto/what-to-do-when-sim-swapping-happens-to-you-1367f296ef4d

[22] https://techcrunch.com/2017/09/18/ss7-coinbase-bitcoin-hack-2fa-vulnerable/

cryptocurrency holder takes appropriate action to eliminate vulnerabilities that are unacceptable and reckless in light of the unique risks associated with holding digital assets.

52. For example, if all U.S. financial institutions suddenly announced that their customers' checking and savings accounts were no longer insured, and that centralized protections have vanished so that unauthorized bank transactions could no longer be reversed (thus exposing their customers' US dollar holdings to the sort of risks attendant to holding cryptocurrency), you would expect some (if not many) of those customers to take some time to ensure they had adequately protected their online access to those access by, for example, not re-using passwords, setting up adequate 2FA, and researching other ways to properly secure their various accounts and holdings. That would be a responsible thing to do in light of the new risks presented in that hypothetical. A common denominator between "traditional" cybercrime and cryptocurrency-related cybercrime is that it is, in fact, quite rare that people who invest a few hours into their cybersecurity fall prey to hackers. Hackers prefer soft targets.

53. It was impossible to be involved in the digital assets space in late 2017, and *especially* in 2018, without hearing about SIM-swaps and cryptocurrency losses. The coverage by press, including well-publicized reports from multiple outlets,[23] as well as posts on social media and panels at conferences, collectively put this issue right in the faces of digital asset participants — all before any of the unauthorized SIM swaps Mr. Williams alleges in this case.

54. Responsible cryptocurrency participants heeded the warnings about unauthorized SIM swaps, which I attribute to the sharp decrease in SIM-swap-related cryptocurrency theft reported to my firm in 2019 and 2020. Undoubtedly, many cryptocurrency users still experienced an unauthorized SIM-swap, but the responsible participants properly secured their critical accounts

[23] *See, e.g.*, **Exhibit C** - SIM-Swapping Articles.

by eliminating the ability to access those accounts via their mobile phone number. In most cases, this involves taking a matter of minutes to download and use Google Authenticator, remove "SMS password reset" features from those accounts, and/or unlinking their mobile phone numbers from those accounts, and/or (for services offering only SMS authentication) using a VoIP service such as Google Voice, which cannot be SIM swapped if properly secured. These responsible users also would have properly secured their credentials to these accounts by, for example, not reusing passwords across multiple accounts, employing password managers and TOTP 2FA, and following instructions to write down (and never store online) any seed phrases or account recovery codes. Taking such measures — which often requires minutes of time per account — insulate those accounts from being accessed by a hacker who takes control of the account holder's mobile phone number.

55. Knowing what safeguards are available is equally as important as knowing the risks you should safeguard against. A responsible participant does not allow FOMO (an acronym for "fear of missing out" commonly used in the cryptocurrency industry) to cause him to blunder haphazardly into the latest blockchain-related trend, but instead takes the time to research and understand the technology in which he will be investing, its vulnerabilities, and how it can be secured against known forms of attacks.

56. For example, a responsible new entrant into cryptocurrency mining would take the time to research the process and, at a minimum, identify the most critical security risks — such as having his mining proceeds diverted to a wallet he doesn't control — as well as the ways to guard against those risks. In this case, Mr. Williams admitted (during a podcast interview he gave after the incident) that he was unaware his Slush Pool mining account had an option to "lock" the wallet

address where his mining payouts were sent,[24] and which could not be unlocked by hackers who gained access to his account. Utilizing this option would have prevented the alleged diversion of 0.23 Bitcoin from Mr. Williams' mining operation,[25] but Mr. Williams apparently didn't take the time to learn what security options were available to him.

57. There is always a tradeoff between convenience and security. More of one typically equates to less of the other. While it may be extremely convenient to simply click "forgot password" and immediately receive a text message code that allows you to access your email account, that is a reckless personal security practice with respect to cryptocurrency. A responsible user achieves the appropriate balance of convenience and security. What is an appropriate balance for someone with only $500 in cryptocurrency may not be appropriate for someone with $5M of cryptocurrency. It may be the case that having adequate security requires an extra few seconds of work to open up the Google Authenticator application and type in the 2FA code to access cryptocurrency, but a responsible user recognizes that extremely minor inconvenience keeps his/her accounts safe from unauthorized access and theft.

B. Practicing good cyber hygiene.

58. A responsible participant also recognizes the elevated risk of cyberattacks that arises from publicly disclosing details of their digital asset activity, such as specifics regarding what platforms they use, their holdings on those platforms, or especially combinations of that sort of information that would make them an attractive or soft target for hackers, and will refrain from doing so. In its simplest form, this is the well-known rule of "don't overshare." Even if digital assets participants feel compelled to publicly disseminate information that could aid a cybercriminal in targeting or

[24] https://podcasts.apple.com/us/podcast/jason-williams-co-founder-partner-at-morgan-creek-digital/id1434060078?i=1000447994515; ATT-WIL-02317.

[25] Compl. ¶ 42.

successfully attacking them (whatever the motivation to do so), a responsible actor would allocate a commensurate amount of time to ensuring his or her personal security measures and practices are sufficient to defend against the increased attention from cybercriminals that will inevitably result.

59. HNWIs, influencers, companies, and anyone else that would be perceived as a more attractive target to hackers have more reason to pay attention to their cyber hygiene and cybersecurity. A common topic of discussion in the industry is not flaunting your wealth,[26] as this type of activity may result in being targeted. If an industry participant does elect to publicly disclose his holdings or show off his cryptocurrency wealth, then the responsible thing to do is to first ensure (either by spending a modest amount of time, money, or both), he has followed all the security instructions applicable to those holding, and has implemented appropriate safeguards against the malicious actors that "wealth flaunting" will undoubtedly attract. The saying "an ounce of prevention is worth a pound of cure" is well-known[27] in broader (not specific to blockchain) cybersecurity. Certainly, one would expect "faces of the industry," such as influencers or those with well-known companies, to have better cybersecurity than what I often refer to as "Joe Retail" — the average person that invests perhaps a few thousand dollars into digital assets.

60. The blockchain industry has many influencers that leave an impression on hundreds of thousands of their followers. Good cyber hygiene entails practices that not only avoid needless risk to oneself, but also to their followers and others with whom they have a digital relationship. To that end, the responsible influencer realizes they have a professional and social responsibility to protect not just their digital assets, but their accounts. The responsible influencer realizes that if, for example, their Twitter account is compromised, the hacker that gained access could potentially

---

[26] https://news.bitcoin.com/stay-safer-by-keeping-your-bitcoin-business-to-yourself/

[27] https://www.ascentor.co.uk/2016/04/ounce-prevention-worth-ton-cyber-attack-cure/

defraud any number of their hundreds of thousands of followers via impersonating them. The responsible influencer would not only care about their followers, but their professional reputation — and, thus, whether out of concern for others, themselves, or both, would spend the few minutes necessary to properly secure these highly valuable social media accounts.

61. The responsible participant realizes that many documents utilized for onboarding in financial services (such as utility bills and digital copies of identity documents/passports to complete know your customer ("KYC") processes) could be utilized to defraud others (impersonation fraud) or to access accounts (via delayed reset) or open accounts in their name. The responsible participant thus secures these documents with an appropriate degree of care. In the event these documents become compromised (which is possible by no fault of the participant — such as an exchange being hacked), the responsible participant notifies the applicable government agency/agencies in order to protect themselves and others, even if it will take them some time to fill out paperwork and get new identity documents, because it's the responsible thing to do. Especially in cryptocurrency, the ramifications of, for example, a selfie with an identity card being stolen by a criminal could include account reset compromises (much like the Coinbase account compromise Mr. Williams experienced), accounts being opened in their name, or others being defrauded via impersonation.

IV. ANALYSIS OF ALLEGATIONS AND EVIDENCE

A. Mr. Williams' background and conduct regarding cryptocurrency, mining, and security.

62. The complaint alleges Mr. Williams was an "early cryptocurrency investor and enthusiast"[28] but does not specify when Mr. Williams first became involved with cryptocurrency. A brief search

[28] Compl. ¶ 8.

of Mr. Williams' Twitter history suggests that Mr. Williams may have first gotten involved with cryptocurrency in 2016, and his response to Interrogatory No. 10 confirms this.[29]

63. Mr. Williams' involvement with cryptocurrencies as early as 2016 establishes he had ample time to conduct responsible research and efforts regarding risks and security for his digital assets and mining operation, including the risk of SIM swaps and using a mobile phone number as a single point of failure. He claims to have "a significant social media presence, where he frequently discusses cryptocurrency news and developments." If this is true, then he was undoubtedly aware of the risk of SIM swaps and vulnerabilities of SMS password reset prior to the first SIM swap, which was a widely-covered topic in the industry before any of the incidents in this case.[30]

64. Consistently, Mr. Williams alleges that as soon as his phone went dead the first time on November 5, 2018 he "suspected a SIM swap attack was occurring,"[31] demonstrating he already knew about SIM swap attacks, how they operated and the risk they presented of a criminal taking control of your phone number — before that first incident.

65. Mr. Williams claims he is "a leader in the field of cryptocurrency markets and security," and "endeavors to stay up-to-date with the latest cryptocurrency news and developments."[32] If this is true, it is effectively impossible that Mr. Williams was unaware of security risks and best practices frequently shared as content on all major cryptocurrency news outlets. It would also be impossible for Mr. Williams to not have known his own personal security choices and practices were inadequate. Not only did he elect to use what is likely the most insecure security option available (SMS password reset) on his "highly sensitive personal and financial"[33] accounts, he persisted in

---

29 Plaintiff's supplemental response to Interrogatory No. 4 (Oct. 1, 2020).

30 *See, e.g.*, articles in Exhibit C.

31 Compl. ¶ 37.

32 Plaintiff's response to Interrogatory No. 10 (July 6, 2020).

33 Compl. ¶¶ 1, 44

doing so despite alleging that same inadequate security setting is what allowed hackers to repeatedly access those accounts.[34]

66. At various points in the litigation, Mr. Williams has claimed his private accounts required SMS "two-factor authentication" or "two-step authentication,"[35] but his descriptions of those processes indicate what he had actually enabled on those accounts was SMS as a *password reset measure* — something entirely different. True SMS 2FA on an account would require Mr. Williams to enter his correct password (1st factor — something you know) and also a code sent via SMS (2nd factor — something you have, although SMS is not a secure or reliable indicator of that) before he could access the account. In his complaint, Mr. Williams describes SMS 2FA as something that allows account access "without a password."[36] It therefore appears Mr. Williams does not have a complete understanding of what two-factor authentication is. This is one of many observations I make in this report that prevent me from agreeing that Mr. Williams held any particular expertise or was a leader in security issues, as he has claimed.[37]

67. Regarding his cryptocurrency mining operation, Mr. Williams' election to start a Bitcoin mining operation in February 2018 suggests he may have done so in light of the crash of Bitcoin's exchange rate.

68. Even for a cryptocurrency beginner, mining Bitcoin can be done responsibly if one educates themselves on the risks and available security options, and uses that knowledge to set up a secure and responsible operation. The information and means to do so was available online well before Mr. Williams commenced any mining activities, including via (among countless other

---

34 Plaintiff's response to Interrogatory No. 3 (July 6, 2020).

35 *See, e.g.*, Comp. ¶ 27; Pl's response to Interrogatory No. 2 (July 6, 2020)

36 Compl. ¶ 27.

37 *See, e.g.*, Plaintiff's response to Interrogatory No. 10 (claiming "Plaintiff is a leader in the field of cryptocurrency markets and security.") (July 6, 2020).

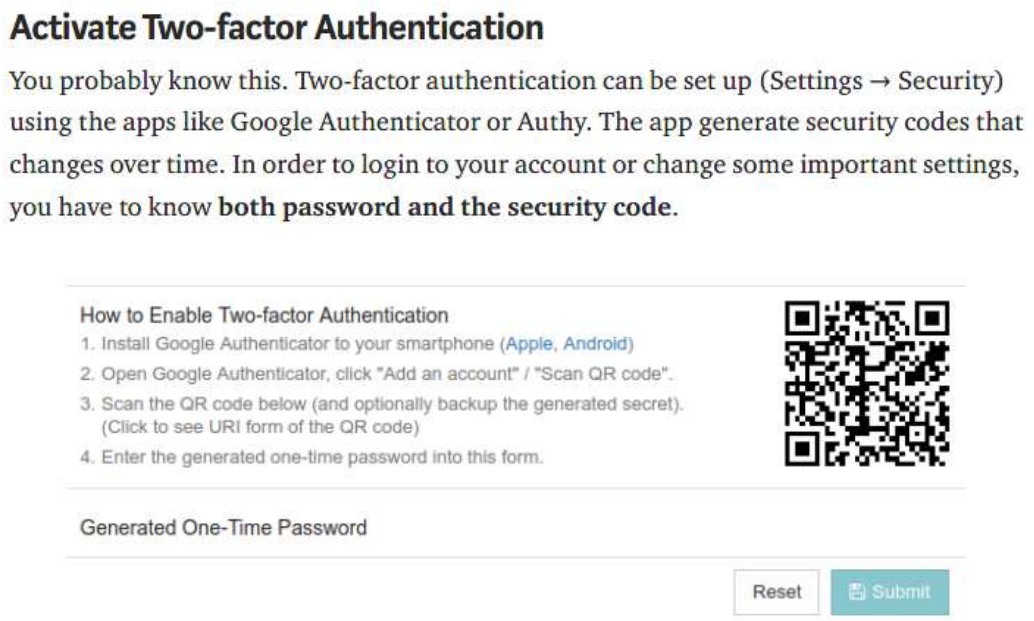
sources) a set of instructions published by Mr. Williams' own mining service, Slush Pool, which is described as a "3 min[ute] read" requiring "low effort" to implement[38]:

Keep Your Slush Pool Account Safe

Slush Pool Follow
Sep 27, 2017 · 3 min read

Internet security is a very complex field. However, sometimes you can achieve fairly high level of security with quite a ***low effort****. It is no different on Slush Pool. Please take a few minutes to read this article and make sure your Slush Pool account is adequately protected.*

69. Slush Pool instructs all Slush Pool miners to employ the same fundamental security practices I associate with a responsible cryptocurrency participant — namely, eliminate a single point of failure by, at a minimum, activating a secure form of 2FA like Google Authenticator:



Activate Two-factor Authentication

You probably know this. Two-factor authentication can be set up (Settings → Security) using the apps like Google Authenticator or Authy. The app generate security codes that changes over time. In order to login to your account or change some important settings, you have to know **both password and the security code**.

How to Enable Two-factor Authentication
1. Install Google Authenticator to your smartphone (Apple, Android)
2. Open Google Authenticator, click "Add an account" / "Scan QR code".
3. Scan the QR code below (and optionally backup the generated secret). (Click to see URI form of the QR code)
4. Enter the generated one-time password into this form.

Generated One-Time Password

Reset Submit

[38] "KEEP YOUR SLUSH POOL ACCOUNT SAFE," Slush Pool (Sept. 27, 2017), Exhibit C.

Had Mr. Williams followed this instruction and properly setup TOTP 2FA, criminal SIM swappers who took control of his phone number would not be able to access his Slush Pool account.

70. Slush Pool also advised its miners to consider employing Slush Pool's basic security feature of "locking" their payout address (the wallet address where their BTC mining rewards are deposited), so that even if an attacker hijacks their account, he or she will not be able to steal their rewards:

> **Set & Lock Your Payout Address**
>
> Firstly, do not forget to set up your payout address. Secondly, consider locking it (Settings → selected coin → Payouts). This is really straightforward and powerful feature. Even if the attacker hijacks your account and bypasess different security measures including 2FA, he **cannot change the payout address** and steal your rewards, as long as he has no control of the specified address.

Had Mr. Williams followed *this* instruction, even if he ignored the preceding instruction to activate TOTP 2FA (which he did), the hackers would not have been able to divert the alleged 0.23 BTC.

B. Mr. Williams' cyber hygiene.

71. Over 138,000 people follow Mr. Williams on Twitter,[39] and certainly countless others have reviewed what he posts. Beyond ensuring — through frequent posts about his cryptocurrency wealth — that cybercriminals would aggressively *target* him, his posts also broadcast information that made it more likely those criminals could *successfully do so*. For example, Mr. Williams would post details known to be utilized by hackers, including specifics on his flight information.[40] Worse, he broadcast the identities of the exchanges where he stored his cryptocurrency (Binance &

---

[39] https://twitter.com/GoingParabolic.

[40] *See* Exhibit B at p. 9. This type of information is utilized by hackers in order to maximize their "time on target" -- if their victim was asleep on a flight, or traveling overseas, it would be less likely the victim would notice and it would be more likely that the hackers could have a longer period of time to obtain the information and access to accounts required to maximize the results of their crime.

Gemini, *see* Exhibit B at pp. 26-27), the wallet address he used (*id.* at p. 29) and told the world that his mining operation is controlled by his Slush Pool account (*id.* at p. 33), thus providing a roadmap to would-be hackers. He further broadcast that he had accounts with Gmail and Authy (*id.* at p. 32), and that he receives his cellular service from AT&T (*id.* at p. 25).

72. Exposing your crypto holdings by transferring funds from an exchange to a wallet and back for the sole purpose of "flexing" on Twitter (and showing a would-be hacker a wallet address and an exchange to look for), exhibits reckless cyberhygiene. Further, this type of activity by Mr. Williams is the only sharing of Mr. Williams' personal information that could aid hackers that I have observed in this case.

73. Mr. Williams also posted information that placed himself (and potentially his family) at risk of physical (not just digital) crime.[41] If someone holds (self-custodies) at their residence, as one example, gold bullion, you would presume they have a safe and adequate home security, amongst other measures, to secure it. Digital assets, as explained above, follow a similar set of expectations. Despite this, Mr. Williams' flaunting of his wealth transcends putting his digital assets at risk. Flaunting the presence of bullion in his home alongside computer screen information that can be used as a timestamp, when it is extremely easy to find his home address, could tempt a robbery.

74. Mr. Williams also did not take preserving identity documents seriously.[42] Even without the information page opened, photos showing a target holding a passport could be used for fraud.

75. Mr. Williams' social media activity also potentially endangered others he engaged with, unrelated to the SIM-swaps. Take for example his Tweet sharing the location where numerous HNWIs would be during a cryptocurrency conference.[43]

---

41 *See, e.g.*, Exhibit B at p.2.

42 *See* Exhibit B at p. 3 (posting a photograph of his face and passport).

43 Exhibit B at p. 4.

76. Beyond the information Mr. Williams publicly disclosed that would assist hackers in targeting him, the hackers who targeted him most likely already knew at least his phone number and, in likelihood, at least one of his email addresses. Via less than one minute spent querying Mr. Williams in TruthFinder,[44] it was possible to identify large amounts of potential personal and personally-identifying information for Mr. Williams.[45] Hackers have no need to go to a company like AT&T for such information, nor would they, as attempting to extract personally-identifying information about an AT&T subscriber would only needlessly increase the risk of their scheme not succeeding.

77. Mr. Williams' personal information, including data such as passwords from past breached accounts, was also easy to access on DeHashed.[46] This further identifies publicly available information that would benefit hackers' efforts to target him — including email addresses he uses and information on passwords he has used for other accounts that were exposed in a data breach — entirely independent of any interaction with AT&T.

V. OPINIONS

A. Mr. Williams exhibited reckless cyber hygiene that caused cybercriminals to target him and gave them tools to do so more effectively.

78. As explained above, Mr. Williams' frequency of Tweeting about his wealth, cryptocurrency assets, and luxury possessions undoubtedly attracted the attention of cybercriminals and led to the aggressive period of SIM swap attempts on his AT&T account.

---

[44] TruthFinder is a publicly available research tool used to pull up contact information and other information for a given person, which costs under $30 per month.

[45] Exhibit E.

[46] Exhibit D. DeHashed is a publicly available tool that costs $15.49 per month and provides a database of breached account information from hacked services. While having information on DeHashed does not, in and of itself, denote poor cyber hygiene, it does identify a potential habit of credential re-use.

79. Making matters worse, Mr. Williams advertised information that would aid hackers both in targeting him and maximizing their ability to compromise his third party accounts. As explained above, his Tweets would disclose his whereabouts and travel plans, what mobile carrier he used, the identity of his cryptocurrency wallets, exchange accounts, mining service, and addresses he used to store his funds, what email service he used, and what TOTP security services he used or may have been using. All of this type of information is known to be used by hackers to more effectively attack a target.

80. Mr. Williams has effectively built a personal brand off of flaunting his wealth and cryptocurrency activity. But building a personal brand off promoting one's net worth requires securing that net worth. While Mr. Williams invested significant time into promoting himself in this manner, it appears he put very little time into properly securing his accounts that would be increasingly targeted as a result of this activity.

B. Mr. Williams disregarded known risks and his own knowledge that he would be targeted by criminals.

81. As soon as his phone went dead the first time on November 5, 2018, Mr. Williams suspected a SIM swap attack was happening.[47] Thus, Mr. Williams was aware of the risks of unauthorized SIM swaps and knew how to prevent the types of harm that could result — before any of the SIM swap incidents he alleges in this case.

82. Moreover, in an interview Mr. Williams gave no later than January 1, 2019,[48] he confirmed he was aware of the threat of SIM swaps, and the article resulting from that interview referenced using TOTP as a way to safeguard against SIM swap-related attacks.[49]

---

47 Compl. ¶ 37.

48 https://blockpublisher.com/sim-swap-attacks-pose-a-serious-threat-to-your-hot-wallets-crypto-linked-accounts-stay-alert/

49 *See* Exhibit B at pp. 14-15.

83. Mr. Williams also knew he could be targeted for SIM swapping by cybercriminals.

84. Upon the first SIM swap incident on November 5, 2018, Mr. Williams claims he informed AT&T that he is a "financial manager" involved with cryptocurrency trading and that he is "at heightened risk of SIM swap attacks."[50] By Mr. Williams' own admission, he was aware by approximately November 5, 2018 (and undoubtedly prior to that) that hackers would likely target or were actively targeting his cell phone number for SIM swap attacks in order to attempt to access his cryptocurrency and other third-party accounts.

85. Given that knowledge, a high-figure cryptocurrency participant or security expert, as Mr. Williams claims to be, should have taken immediate action to easily defeat that risk.

C. Mr. Williams employed reckless and inadequate cybersecurity practices.

86. Despite his knowledge of SIM swap risks and that he would be targeted, and despite AT&T's disclosures that it could not guarantee the security of his AT&T account,[51] Mr. Williams employed reckless and inadequate security practices that could allow a successful SIM swap attack — particularly when aided by the types of private information Mr. Williams advertised on social media — to result in the compromise of his private third-party accounts.

87. Mr. Williams could have taken numerous, simple steps to safeguard those accounts in the event he was successfully SIM swapped, with some examples being adding TOTP or hardware-key 2FA, removing SMS password reset, using wallet whitelisting, using a properly-secured VoIP or Google Voice phone number, or simply locking a payout address. A responsible person — and certainly someone who claims to be a "leader in the field of . . . security"[52] and held as much

---

50 Compl. ¶ 47.

51 *See, e.g.*, AT&T Privacy Policy, ATT-WIL-01591-92 ("no security measures are perfect, we cannot guarantee that your Personal Information will never be disclosed in a manner inconsistent with this Policy"); Wireless Customer Agreement, ATT-WIL-05974 ("AT&T DOES NOT GUARANTEE SECURITY").

52 Plaintiff's Response to Interrogatory No. 10 (July 6, 2020)

cryptocurrency as Mr. Williams advertised he did — should have done at least some, and probably most or all, of these.

88. Instead, and despite the warnings issued by Slush Pool and others, Mr. Williams elected to enable SMS *password reset* (not SMS 2FA as he incorrectly claims) — the very feature that illicit SIM swaps principally seek to exploit — on his Google account (and others). He did this despite also knowing that anyone who compromised his Google account could thereby gain access to what he describes as his other sensitive financial and business accounts, including his Slush Pool mining account and the accounts where he alleges he stored his own sensitive personal information and that of his family members. In short, he set up the security on all of the accounts at issue to be as susceptible as possible to a criminal who took control of his phone number.[53]

89. However, the accounts that he alleges were compromised were not all of his important accounts. For instance, before the first SIM swap, the criminals who targeted him undoubtedly knew he likely kept large amounts of cryptocurrency in a Gemini and/or Binance exchange account.[54] Yet Mr. Williams does not allege his Binance account was compromised and he only alleges criminals "attempted" to access his Gemini account.[55] The most likely explanation for why the perpetrators of the SIM swaps did not get into those two accounts is that Mr. Williams knew how to enable, and in fact enabled, security measures on those accounts which did not permit access via control of his phone number.

---

[53] *See* Plaintiff's response to Interrogatory No. 3 (stating all of his compromised accounts were set up to have their passwords reset via an SMS message, or could otherwise be accessed via his Google account which could have its password reset via an SMS message) (July 6, 2020).

[54] *See, e.g.*, Exhibit B at pp. 28, 30 (Aug. 12, 2018 Tweet from Mr. Williams disclosing his Gemini account and its holdings; Apr. 28, 2018 Tweet from Mr. Williams disclosing his Binance account).

[55] Compl. ¶¶ 52, 55, 60.

90. In fact, records produced by Coinbase indicate Mr. Williams enabled TOTP on his Coinbase account as early as November 13, 2018.[56] Yet he chose not to do so for his other accounts like Google and Slush Pool.[57] Based upon Mr. Williams' document production and discovery responses,[58] it is unclear whether he utilized Authy or Google Authenticator for TOTP on his Coinbase account. If he utilized Authy, this may suggest he disabled Authy's multi-device feature prior to his Coinbase account compromise. If Mr. Williams utilized Google Authenticator for TOTP on his Coinbase account, he already had the very app needed to keep his other accounts (including his Google and Slush Pool) easily secured. In either case, and in another example of Mr. Williams taking steps to undermine his own security, Mr. Williams defeated the point of this TOTP protection by keeping identity documents such as images of the front and back of his driver's license online (in a non-TOTP secured location) that could be used to reset those protections.

91. But what is most baffling — and troubling — about Mr. Williams' conduct is his refusal to change his security configuration after each of the multiple breaches of his accounts, despite his belief that his security configuration is what the hackers repeatedly exploited to gain access to his accounts.

92. Following the first (Nov. 5, 2018) incident, Mr. Williams was aware that his phone number being SIM-swapped could lead to a password reset for his Google account, which could also give

---

[56] See "jasonwilliamseow@gmail.com Compliance Report.csv" (data later labeled as COINBASE_000003).

[57] *See infra*, fn 58. Documents produced by third party Gemini also indicate Mr. Williams attempted to use Authy (another form of TOTP 2FA) to secure his Gemini account, but that Mr. Williams claimed the attackers "hacked" his Authy account as well. GEMINI_0008. The only way hackers could remotely access his Authy account is if Mr. Williams affirmatively enabled Authy's multi-device feature *and then left it in place* – against Authy's "strong[] suggest[ion]" to disable it. ATT-WIL-02152.

[58] *See, e.g.*, Plaintiff's response to Interrogatory No. 2 (July 6, 2020) (no discussion of any TOTP usage on any account); Plaintiff's supplemental response to Interrogatory No. 2 (Oct. 1, 2020) (same).

hackers the ability to access his other sensitive accounts. There were several simple things Mr. Williams could and should have done in response to this first attack (which I have outlined above) that would prevent the recurrence of any breach of his third party accounts following a future SIM swap.

93. Yet Mr. Williams claims in his interrogatory responses that all he did after that first incident — and after each subsequent incident — is change the passwords to his accounts, despite articulating in those same interrogatory responses precisely why merely changing passwords would do nothing to prevent future breaches of those accounts by anyone who took control of his phone number, so long as he continued to enable SMS password reset.[59]

94. And this is, in fact, what Mr. Williams alleges happened: in each subsequent incident, he claims the hackers accessed his private accounts "by using the same methods [they] used [the first time.]"[60] In other words, he believed the hackers repeatedly exploited the same inadequate security settings he chose to implement, yet elected to maintain those same settings following each incident. In all the cybercrimes I have investigated, I have never observed such a pattern of easily avoidable recurrences.

95. Instead of taking mere minutes to set up Google Authenticator on *all* of his accounts,[61] Mr. Williams sought to obtain assurances of special treatment from employees at an AT&T retail store in Raleigh, NC. Mr. Williams alleges he relied on statements by those store employees that extra security would be added to his account, and that future requests for SIM changes would have to

---

59 Plaintiff's responses to Interrogatories Nos. 2 & 3 (July 6, 2020).

60 Plaintiff's responses to Interrogatory No. 3 (July 6, 2020).

61 Mr. Williams' Coinbase account evidences his use of TOTP, meaning Mr. Williams had already downloaded the prerequisite application and was familiar with how to add TOTP to accounts. Consequently, adding the same level of security for his other accounts, such as Google and Slush Pool, would have been a trivially quick matter of scanning a QR code and entering several digits to confirm. *See* Exhibit B at p. 19.

be made in person and with two forms of identification. Mr. Williams knew or should have known that these measures could not guarantee he would not be SIM swapped again.

96. By November 2018, it was widely reported in news media online that such measures cannot guarantee a SIM swap will not happen, particularly if it is done by an insider.[62] Yet after each incident, Mr. Williams chose not to make any changes to his personal security practices and instead elected to rely on his mobile phone carrier as the single point of failure for the protection of his private third-party accounts.

97. Mr. Williams had the information, means, ability, and responsibility to properly secure his private accounts with third parties. He could have done this in a fraction of the time he spent asking AT&T to place notes on his account requesting bespoke security procedures.

D. The SIM swaps did not provide hackers with a "mirror image" of Mr. Williams' phone.

98. Mr. Williams' allegation that the hackers who targeted him "were also able to create a 'mirror image' of his phone"[63] is almost certainly untrue and, in any event, I have not identified anything in his document production (JW_0001-75) that would corroborate that allegation.

99. The unauthorized SIM swaps did not and cannot provide a backup of Mr. Williams' iPhone. The only way a hacker could obtain a mirror image of Mr. Williams' phone would be if Mr. Williams elected to store an unencrypted backup of his device on one of the services that he alleges these hackers accessed (or an encrypted backup with the password to unlock that encryption within one of those improperly-secured services).

---

62 *See, e.g.*, https://www.flashpoint-intel.com/blog/sim-swap-fraud-account-takeover/ (published June 8, 2018, detailing campaigns by hackers to target mobile store employees and pay them to perform SIM swaps); https://www.wired.com/story/sim-swap-attack-defend-phone/ (published Aug. 19, 2018; describing recruitment of phone company employees and stating "[i]f a skilled SIM hijacker targets you, there's realistically not much you can do to stop them;" and stating SMS 2FA "won't help at all if a SIM swap hits") (underline in original).

63 Compl. ¶ 40.

100. Mr. Williams' Response to Interrogatory No. 2 does not list his Apple/iCloud account — the account where a backup of his phone's memory would be stored — as one of the accounts hackers breached. Consequently, the *only* way hackers could have created a mirror image of Mr. Williams' phone was if Mr. Williams stored a backup of his device on one of the improperly-secured file storage service that he alleges was breached (*e.g.*, Google Drive, DropBox, etc.). Again, I have seen nothing in Mr. Williams' discovery responses or the documents he produced to indicate this happened or otherwise support his allegation that hackers obtained a mirror image of his phone.[64]

101. Accordingly, Mr. Williams is incorrect when he alleges a SIM swap enabled hackers to identify the accounts where "he most likely had money or cryptocurrency."[65] To the contrary, neither AT&T nor the SIM swaps themselves informed the hackers where Mr. Williams kept his cryptocurrency. Mr. Williams did that by failing to properly secure that information or publicly advertising it on his Twitter account. It was Mr. Williams who told the hackers what accounts he used and where he kept his cryptocurrency.[66]

E. The materials Mr. Williams has produced do not establish his third-party accounts were compromised due to the SIM swaps, and not some other intervening event.

102. Although Mr. Williams alleges the SIM swaps are what enabled the hackers to breach his third party accounts (Slush Pool, Gmail, Google Drive, Dropbox, Twitter, Instagram, Linkedin, Coinbase, Gemini, First Citizens Bank),[67] the materials he has produced (Bates labeled JW_0001-

---

64 *See, e.g.*, JW_0001-75 (no document indicating Mr. Williams stored an unencrypted backup of his iPhone, or that any hacker accessed a backup of his iPhone); Plaintiff's Response to Second RFPs No. 9 (claiming he does not have records of which of his files or sensitive information hackers alleged accessed, or that he has already searched for and produced any such records he has).

65 Compl. ¶ 40.

66 *See, e.g.*, Exhibit B at pp. 25-31

67 Plaintiff's supplemental response to Interrogatory No. 2 (Oct. 1, 2020).

75) do not establish that is the case, or that his accounts were not breached for reasons independent of the SIM swaps.

103. For example, JW_0058 states the breach of his Coinbase account began on February 3, 2019, when the password on that account "was reset from a Windows 10 device." Mr. Williams has not produced anything establishing that password reset did not result from a vulnerability in Mr. Williams' security practices entirely independent of the SIM swap. Moreover, that same document states the Coinbase breach was completed by, among other things, the hacker providing Coinbase with "photos of the front and back of [Mr. Williams'] ID along with a photo of [Mr. Williams'] face" — things AT&T did not have and could not have provided to the hacker(s), and as evidenced elsewhere in this Report, resulted from Mr. Williams' inadequate protection of his Google account.

104. The Coinbase breach is the only breach for which Mr. Williams' document productions provide any meaningful detail regarding how the breach occurred and, as noted above, still presents numerous unanswered questions as to the cause of or responsibility for the breach. For the other alleged breaches — Google (Gmail/Drive), Slush Pool, Twitter, etc. — Mr. Williams' document productions contain no information that would enable anyone to conclude (without significant speculation) that the SIM swaps, and not some other intervening events/failures, enabled or caused the breaches.

105. For instance, even without a SIM-swap, it is possible that Mr. Williams' jasonwilliamseow@gmail.com may have been compromised via another vector. As one example, his document production shows password reset emails being sent to jwilliams@prtitech.com,[68] which appears to be a recovery email for his Gmail account. If the credentials for the latter email

[68] *See, e.g.*, JW_0053.

were compromised, by proxy, the former account would be compromised, regardless of whether or not a SIM-swap took place.[69]

106. While I do not know (and cannot know unless Mr. Williams provides evidence) the security settings for each of these email accounts, if Mr. Williams did not have appropriate 2FA on his @prtitech.com account, and reused passwords (which, as per DeHashed, and Mr. Williams' alleged practice of rapidly memorizing entire sets of new passwords, seems entirely possible) — his Google account could have been compromised completely independently of a SIM swap.

107. Further, if Mr. Williams had been a victim of phishing or malware, this same single point of failure would have resulted in access to the array of items described in this action, such as identity documents and other sensitive information/credentials.

108. These same problems of causation present for each of the account breaches that Mr. Williams alleges resulted from a SIM swap.

F. Hackers used Mr. Williams' Google account, not his phone number, to access most if not all of the accounts at issue.

109. In his Complaint, Mr. Williams alleges hackers used their control over his Gmail (more accurately, Google) account to "hack" into his Twitter, Instagram, DropBox, Google Drive, and LinkedIn accounts.[70] And based upon the sequence of events described in Mr. Williams' response to Interrogatory No. 2, I am left to conclude that Mr. Williams' Slush Pool account was also accessed via his Google email account, via a password reset email.

110. Moreover, as described above, Mr. Williams' failure to properly secure his Google account appears to have, in turn, provided the hackers with access to identity documents he ill-advisedly

---

[69] This is what happened to Ian Balina's Google account, and subsequently, his Evernote account, leading to compromise of profit keys by hackers including Joel Ortiz. In that case, Ortiz et al. didn't SIM swap Ian Balina, but simply took advantage of a known compromised password.

[70] Compl. ¶ 39.

uploaded and stored on a non-TOTP-secured Google Drive which, in turn, appears to have enabled those hackers to successfully request a reset of the TOTP-secured Coinbase.[71]

111. Although Mr. Williams has not specified the exact manner in which his Google account was utilized to access all of the accounts that he alleges were breached — whether as a login or through a password reset email — his allegations and discovery responses make it clear that hackers used Mr. Williams' *Google* account, not his *phone number*, to access these services.

G. Mr. Williams' document production does not substantiate the alleged diversion of Bitcoin from his mining operation.

112. Mr. Williams alleges that the hackers who breached his Slush Pool account in November 2018 diverted 0.23 BTC from that account. To date, Mr. Williams has not produced records from his Slush Pool account to corroborate that allegation. While Mr. Williams has produced an email[72] indicating a belief that hackers used a wallet address beginning with "3FSC" to divert those funds, which wallet received approximately 0.44 BTC in November 2018, it is impossible to determine if those funds (or any funds) were in fact diverted from Mr. Williams' Slush Pool account absent corresponding records from Slush Pool.

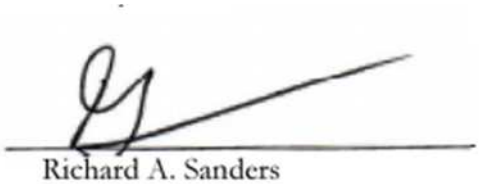
113. I reserve the right to provide additional information regarding these opinions and / or further opinions if asked to do so by AT&T or in response to newly-discovered information, or as necessary for rebuttal purposes.

---

71 JW_0058.

72 JW_0065.

// ENDS



Richard A. Sanders
Lead Investigator, Principal
CipherBlade

EXHIBIT A

CipherBlade
Blockchain Investigation Agency

+1 (732) 890-7874
rich@cipherblade.com
www.cipherblade.com

Curriculum Vitae of **Richard Sanders, CRC**

Forensics reports, Declarations, and other work samples available upon request and NDA signing.

Summary: Combat veteran continuing a sense of mission as a blockchain forensics expert and cryptocurrency cybercrime investigator with experience in dozens of cases. Seen as subject matter expert by legal, law enforcement, and regulatory professionals. Experience working with top law firms performing forensics work and other expertise-based supportive efforts. Experience testifying and writing reports for a diverse array of cases involving cryptocurrency, including OTC deals, theft (as one example, SIM-swaps), and suspect ICO (misappropriation/embezzlement/etc.) disputes. Strong leadership, investigative, and analytical skills foster results.

CipherBlade: Lead Investigator, Co-Founder

- Launched first-of-kind cryptocurrency investigative agency
- Leads team of 8 staff dedicated to uprooting fraud and discovering the truth via the blockchain
- Renowned expert in blockchain forensics (utilizing tools such as Chainalysis, Crystal, or tools developed internally by need,) briefing law enforcement, legal professionals, and senior level exchange executives/compliance staff on complex blockchain transactions, security vulnerabilities, and other rapidly evolving elements of new waves of crime
    - First Certified Investigative Partner with Chainalysis
- Expert witness with experience leveraging deep knowledge of cryptocurrency criminal methodologies and networks
    - Maintains active infiltration in underground hacker/scammer communities to maintain cutting edge threat intelligence leveraged by AML professionals and law enforcement
    - Developed and maintains list of common tendencies/observations of suspicious blockchain companies, which have provided 100% accuracy in data points upon reviewing ICOs/equivalent for mismanagement, embezzlement, and other crime
    - Serves as trainer and mentor for professionals in the public and private sector regarding fusion of on-chain and off-chain intelligence, leveraging OSINT and other techniques with blockchain forensics expertise to foster an environment in which “they can’t hide”
    - Has a 100% success rate in unveiling undisclosed cryptocurrencies in divorce cases
- Lead investigator for dozens of cryptocurrency scams and hacks, most notably the ‘OGUsers’ ring with many arrests in 2018
    - As a lead investigator, is involved throughout full case lifecycle, from the time of incident through prosecution
    - Assists affected parties with stabilizing upon breach and gathering initial forensics data
    - Generates law enforcement reports in a renowned “pretty box with a ribbon” format, greatly enhancing likelihood that reports are actionable and serving as a catalyst for law enforcement action on highly complex cases that often lack past “playbook precedent”

    - Conducts investigation of person(s) of interest for such incidents, including social engineering of social engineers, and feeding identifying data to law enforcement which led to the arrests of many simswappers via REACT and the FBI
    - Assists prosecutors by feeding evidence and opinion in order to ensure person(s) responsible for these incidents are held appropriately accountable
    - Assists victims and legal counsel by generating Declarations, often enabling and expediting asset recovery after arrests and asset seizure
- Advisor for top-tier blockchain projects, such as Dusk and ChromaWay
- Leverages blockchain, regulatory, and cyber knowledge to serve exchange clients such as Bitbuy with solvency audits
- Provides public-facing expert research and opinion on controversial matters in the blockchain industry, such as the Coinomi vulnerability and ShapeShift/WSJ dispute
- Speaks at events and panels such as Blockchain In The Burgh to raise awareness about the importance of preventative security, AML, and public safety considerations
- Provides insight and training to numerous LEAs on complex issues such as BECs, elder abuse/fraud, romance scams, money mules, and other typologies that require additional external expertise

Crypto Defender's Alliance: Leadership Team

- Selected to be one of five administrators of Crypto Defenders Alliance (CDA), an organization comprised of executives and AML/Compliance/Legal staff from nearly all cryptocurrency exchanges which seeks to thwart fraud involving cryptocurrency
- Observes best practices from work with CipherBlade clients and/or in the course of CipherBlade investigations and fields requests for bleeding-edge insight on complex topics such as mixers beneficial to even well-known, compliant exchanges such as Coinbase
- Led initiative to significantly bolster representation of member organizations in CDA based upon observing a need for representation from a particular continent (Africa), resulting in adding the majority of cryptocurrency exchanges focused in that region and uprooting untold millions in scam laundering
- Manages intra-exchange communication to combat ML and share best practices in the premiere industry self-regulatory organization

Anti-Human Trafficking Intelligence Initiative: Blockchain Forensics and Industry/Law Enforcement Liaison

- Led initiative to significantly bolster representation of member organizations in ATII based upon observing a need for representation from particular cryptocurrency exchange and service typologies, with a special emphasis on P2P trading platforms and exchanges identified in the course of CSEM investigations
- On numerous occasions, acted upon intelligence provided within ATII that included Bitcoin wallet addresses pulled from dark websites soliciting and distributing CSEM. As just one example of efficacy and efficiency, coordinated dusting attack targeting 46 different child exploitation sites (at a $36 self-funded cost and with 15 minutes of effort) which resulted in data able to unveil thousands of CSEM purchasers and identify where the CSEM distributors were laundering funds
- Upon unprecedented results, was asked within months of membership to join ATII's Advisory team
- Participated in Follow Money Fight Slavery 2021 Summit on the Cryptocurrency Kiosk and Bitcoin ATM Panel

Educational Qualifications and Professional Certifications

Mr. Sanders earned a Bachelor of Science degree in Homeland Security while on active duty with the US Army. Despite maintaining a work schedule that far exceeded the typical "9 to 5," he devoted almost the entirety of his off duty hours to utilizing the educational benefits provided to him as a service member to exceed the standard with a 3.7 GPA. He holds numerous awards, affiliations, and memberships in a variety of functional areas, mostly within military and security work as well as philanthropic undertakings. The most notable of these is a CORe credential from Harvard Business School extension. Mr. Sanders holds a Certified Blockchain and Law Professional with the Blockchain Council as well as Certified Bitcoin Professional certification.

Mr. Sanders also holds a Chainalysis Reactor Certification, a course ran by the firm which provides the forensics tool most frequently utilized in blockchain forensics. During this course, Chainalysis staff shared that Reactor is a tool that presents data; analysis is still up to the analyst, and referenced Mr. Sanders as one of the top analysts. Mr. Sanders attended the first Chainalysis CISC course by request and provided immense helpful feedback. Minimal formal training exists for blockchain forensics, and *zero* training exists that covers the full spectrum, marrying on-chain and off-chain observations into a comprehensive skillset. Mr. Sanders has been requested to develop training for CDA, and is in discussions to begin guest lecturing. In short, Mr. Sanders is creating the educational qualifications.

- Certified Blockchain and Law Professional, Blockchain Council
- Chainalysis Investigation Specialist Certification, Chainalysis
- Certified Bitcoin Professional, CryptoCurrency Certification Consortium (C4)
- Chainalysis Reactor Certified Professional, Chainalysis
- HBX CORe, Harvard Business School

Other experience and education available on LinkedIn

Mr. Sanders in Press/Media

Mr. Sanders is in increasing high-demand for quotes for articles, podcasts, and interviews. Below are some of a continually growing list of the aforementioned:

- https://youtu.be/0HHZnFBTESw
- https://www.coindesk.com/cipherblade-okex-huobi-csem-morphtoken
- https://bravenewcoin.com/insights/podcasts/the-blockchain-detective-taking-on-elite-cybercriminals-and-owning-them
- https://thenews.asia/interview-with-rich-sanders-okex-and-market-transparency/
- https://decrypt.co/29865/meet-the-forensics-expert-who-tracks-stolen-bitcoin
- https://www.coindesk.com/crypto-scam-apps-in-app-stores
- https://decrypt.co/17103/forensic-investigator-sudden-shut-down-of-the-coss-exchange-looks-suspicious
- https://cryptobriefing.com/hitbtc-insolvent-scams-users-cybercrime/
- https://anchor.fm/scottcbusiness/episodes/Discussing-Cipherblade-With-Richard-Sanders-ebi2ot
- https://mondovisione.com/media-and-resources/news/chainalysis-launches-certified-investigative-partnership-program-to-meet-demand
- https://www.financemagnates.com/cryptocurrency/news/bitbuy-conducts-third-party-audit-launches-otc-desk/
- https://unchainedpodcast.com/how-to-keep-your-crypto-from-being-stolen-via-your-phone/

Summary of Expert Witness Experience

Carlos Martinangeli v. Akerman, LLP, et al.	LeClairRyan LLP, Counsel for Defendant	Southern District of Florida
Dooga Ltd. v (Numerous)	Kobre & Kim LLP, Counsel for Plaintiff	United States Bankruptcy Court, Northern District of California
Hub Token v. AT&T Mobility LLC, AAA No. 01-20-0000-4297 (arbitration)	Kilpatrick Townsend & Stockton LLP, Gibson Dunn & Crutcher LLP, Counsel for Respondent	Arbitration (pending)
Dibiase v. Bittrex	McNaul Ebel Nawrot & Helgren PLLC, Counsel for Defendant	Arbitration (Deposition)
Moss v. Bittrex	McNaul Ebel Nawrot & Helgren PLLC, Counsel for Defendant	Arbitration

(3 separate cases) Wright v. Defendant	SCA Ontier LLP, Counsel for Plaintiff	Varied English courts
Wang v. Darby	Curzon Green Solicitors, Counsel for Plaintiff	High Court of Justice, England
USA v. Defendant	Confidential	Confidential
Nationstar Mortgage LLC v. Patrick Soria, et al.	Hall Griffin LLP, Counsel for Plaintiff	United States District Court, Central District of California
Park v. Park	Meyer Darragh Buckler Bebenek & Eck, P.L.L.C., Counsel for Plaintiff	Fifth Judicial Circuit of Pennsylvania
Shebeck v. LaFond	Radford J. Smith, Chartered, Counsel for Plaintiff	District Court, Clark County, Nevada (Testimony)
Anatha v. John Doe	Horizons Law & Consulting Group, Counsel for Plaintiff	Pending
Nirvana Capital LTD v. Mobile Gaming Technologies Inc. et. al	Horizons Law & Consulting Group, Counsel for Plaintiff	United States District Court, Northern District of California
Anthony Fasulo & Gautam Desai v. Xtrade Digital Assets Inc. et. al	Kirsh LLC, Counsel for Plaintiff	United States District Court, Southern District of New York
USA v. Matthew Brent Goettsche	Kobre & Kim LLP, Counsel for Defendant	United States District Court, District of Colorado
GSR v. The Fr8 Network	Aaron Krowne, PLLC, Counsel for Plaintiff	Settlement
Matsumoto v. John Does	McNaul Ebel Nawrot & Helgren PLLC, Counsel for Plaintiff	Pending
Williams v. KuCoin et. al	Roche Cyrulnik Freedman LLP, Counsel for Plaintiff	United States District Court, Southern District of New York
Klein v. Kim	Rogers Joseph O'Donnell PC, Counsel for Defendant	United States District Court, Western District of Washington
USA v. Kim	Rogers Joseph O'Donnell PC, Counsel for Defendant	United States District Court, Northern District of California
Powers v. American Crocodile International Group Inc.	Maxwell Goss, PLLC, Counsel for Plaintiff	United States District Court, Eastern District of Michigan
Hershkowitz Shapiro PLLC. v. John Does	Mcdonald Hopkins LLC, Counsel for Plaintiff	Pending
Schwartz v. Haas	Brett Kimmel, PC, Counsel for Plaintiff	Supreme Court of the State of New York
GoxCorp, USA v. (seized assets)	Maxim Price (pro hac vice pending), Counsel for GoxCorp	United States District Court, Northern District of California + Japanese court pending
Confidential	Kostelanetz & Fink, LLP, Counsel for Defendant	Pending

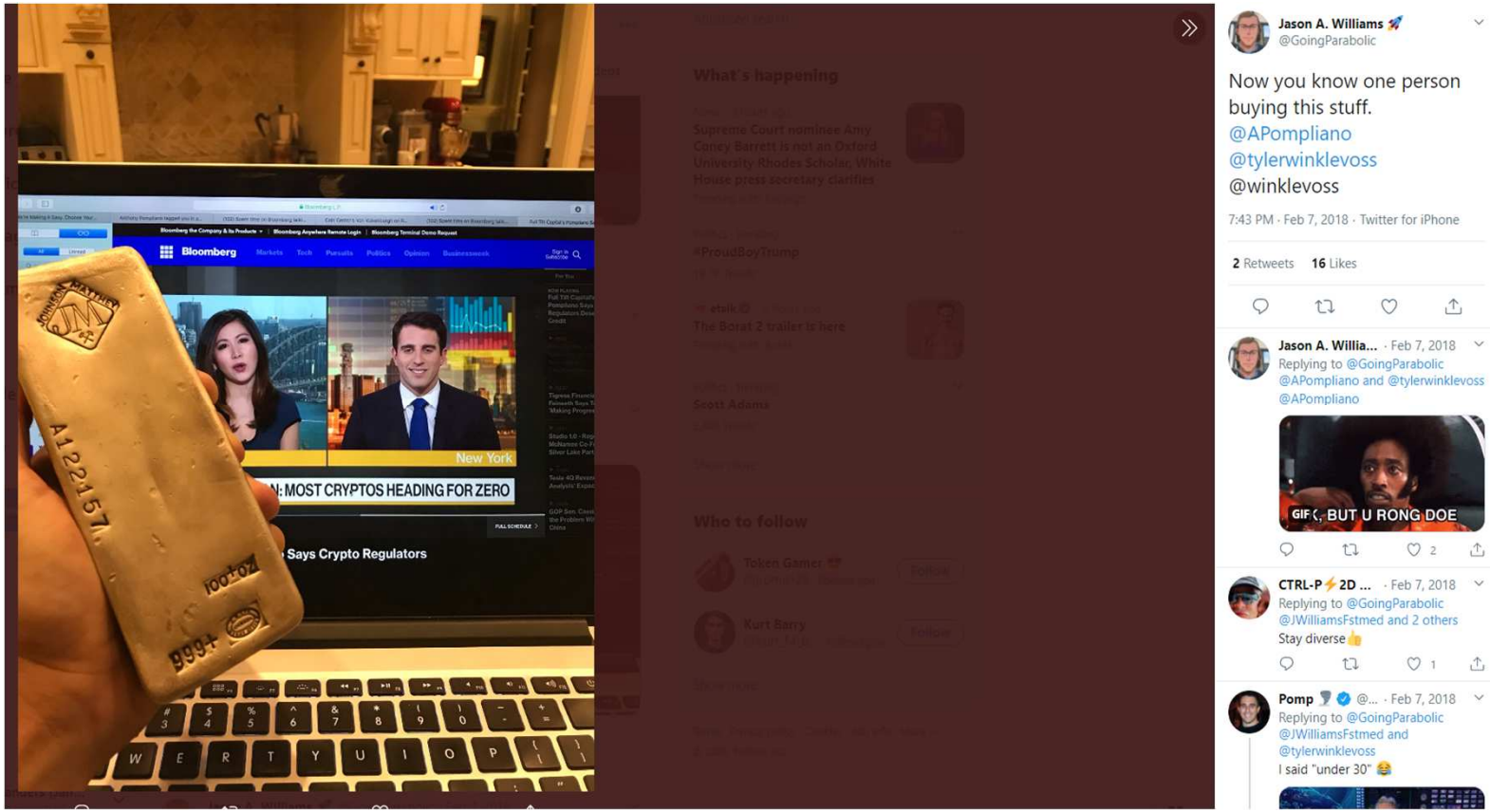
Government of the Cayman Islands v. John Does	CIG, pro se	Pending
USA v. Confidential	Dilendorf Khurdayan PLLC, Counsel for Defendant	Confidential

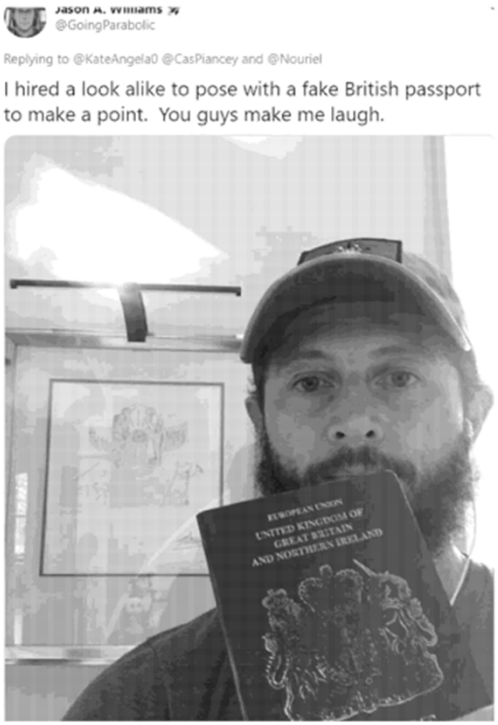
Mr. Sanders has served as an expert for either or both Plaintiff and Defendants in cases involving, as some examples:

- Divorce
- ICO disputes against “soft exits” or other mismanagement
- Cases against ICOs (including Enforcement actions) and VCs/funds
- SIM swapping and other theft
- Cryptocurrency exchange account compromises
- OTC disputes
- Cryptocurrency taxes
- Immigration
- Source of funds
- Misappropriation/embezzlement
- Cryptocurrency exchanges
- Fraud
- Hacks
- AML/Compliance

EXHIBIT B


Follow
Jason A. Williams
@GoingParabolic
Co-founder and partner at Morgan Creek Digital • Started and sold some cool companies • Host of livestream Going Parabolic (link to YouTube below)
Raleigh, NC
youtube.com/c/GoingParabol...
Born March 11
Joined February 2013
543 Following
50K Followers
Followed by VCs Congratulating Themselves, Coinbound, and 140 others you follow


Bloomberg
New York
MOST CRYPTOS HEADING FOR ZERO
Says Crypto Regulators
What's happening
Who to follow
Jason A. Williams
@GoingParabolic
Now you know one person buying this stuff.
@APompliano
@tylerwinklevoss
@winklevoss
7:43 PM · Feb 7, 2018 · Twitter for iPhone
2 Retweets 16 Likes
Jason A. Willia... · Feb 7, 2018
Replying to @GoingParabolic @APompliano and @tylerwinklevoss @APompliano
GIF (, BUT U RONG DOE
CTRL-P⚡2D ... · Feb 7, 2018
Replying to @GoingParabolic @JWilliamsFstmed and 2 others
Stay diverse
Pomp · Feb 7, 2018
Replying to @GoingParabolic @JWilliamsFstmed and @tylerwinklevoss
I said "under 30"



ATT-WIL-02295

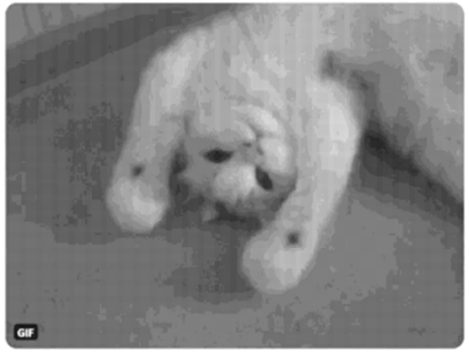
ATT-WIL-02237

This account owner limits who can view their Tweets. Learn more

Jason A. Williams 🚀
@GoingParabolic

Replying to @eatmykarbon

What is happening here. Meme game going litigation. Am I going to get sued for my cat gifs? Maybe a legal disclaimer



1:38 PM · Nov 23, 2018 from Raleigh, NC · Twitter for iPhone

2 Likes

Jason A. Williams 🚀 @GoingParabolic · Nov 23, 2018

Wow. That makes no sense. I'm sorry. Is it some type of cyber bullying or something? All he had to do was just move on. He trapped in meme world?

1 1

ATT-WIL-02290

Jason A. Williams 🚀 @GoingParabolic · Jan 14, 2018

Replying to @polina_marinova

This is why you should never leave your holdings in a trading platform. Move your crypto assets to a secure wallet. Bang Bang...🚀🧠💩

2

ATT-WIL-02226


Jason A. Williams
@GoingParabolic
Unknown Opinion -
10 things that are "Not Great" occurring in the crypto ecosystem Right Now -
1. Bomb threats
2. SIM Swaps
3. Extortion attempts
4. Threats of kidnapping
5. Email Hacks
6. Computer hacks
7. Dark Web theft
8. Swatting
9. Doxxing
10. Hiring Police Protection
6:01 AM · Dec 14, 2018 from North Carolina, USA · Twitter for iPhone
4 Retweets 15 Likes
Ozaps @morebtcplz · Dec 14, 2018
Replying to @GoingParabolic and @JWilliamsFstmed
Hectic! I have not heard of 1, 7, 8,9 or 10? Got articles?
Jason A. Williams @GoingParabolic · Dec 14, 2018
No, but I should probably write a paper on them.

Jason A. Williams 🚀 @GoingParabolic · Aug 9, 2018

Who owns your Twitter account when you kick the bucket? Your Bitcoin? Your IG account?

These things all have value. Are they just lost with the passwords and usernames?

Seems like valuable stuff. Someone should come up with a plan.

16 11 73

Show this thread

ATT-WIL-02263


Jason A. Williams 🚀 @GoingParabolic · Sep 5, 2018
When you arrive at the airport at 3:56 for a **flight** that leaves at 4:10 and you make it. #savageaf
I'm that guy running in the airport. Don't hate me.
GIF
1
19


Linear
Log
EXPORT DATA
10/01/2018 to 04/30/2019
1h 12h 1d 1w 1m 3m 1y all
$6500
$6000
$5500
$5000
$4500
$4000
$3500
coindesk
Oct
Jan
Apr

U2F AUTHENTICATION

Slush Pool Introducing New, Safer and More Convenient 2FA Method — U2F

Braiins | Slush Pool Follow
Sep 13, 2016 · 2 min read

We have made great progress in our continuous effort to protect our customers, even more than we already did! Today, we are proud to release a new type of two-factor authentication method — U2F. It is especially useful for miners who already own hardware devices like TREZOR or YubiKey, because starting today they can use them for 2FA authentication with the pool.


The Coinbase Blog
PRODUCT NEWS
PRO
INSTITUTIONAL
AROUND THE BLOCK
ENGINEERING
UK & EUROPE
How to increase your Coinbase account security
soupsranjan
Follow
Apr 22, 2017 · 6 min read
We advise our users to install Authenticator apps (Google Authenticator, Microsoft Authenticator) as their primary 2FA method to secure their Coinbase accounts from phone porting attacks. You can follow the steps outlined in our support article to use Authenticator.
The instant and irreversible nature of digital currency enables fascinating use cases and drives our mission to create an open financial system for the world. This includes helping merchants accept bitcoin with no chargeback risk and helping users do global remittances instantly at low fees. But that very nature of bitcoin also attracts sophisticated attackers that challenge this mission.

GEMINI Products Prices Security Institutions Resources Sign in Get started

INDUSTRY | PRODUCT | TECHNICAL

Better Two-Factor Authentication (2FA)

Jan 26, 2017

Cem Paya
Security Team

We have required all of our customers to use two-factor authentication (2FA) from day one. In keeping with our security-first philosophy of protecting and educating our customers, we want to provide some background on our 2FA system ***to encourage our customers to use the Authy app for 2FA rather than SMS***, and to dispel some common misconceptions.

Jason: "I was overseas and I was working actually at about 12 AM where I was. I was on my phone and I noticed all of a sudden that my SIM card shut off, I had no service. I immediately went into my settings and it showed that my SIM card had been deactivated. I had known about the sim-swap attacks and doxxing but I had never experienced it. In the next 12 hours, all hell broke loose for me.

SIM swap is a real issue. People need to be more aware of the situation. Personal information linked to your account's security should be kept safe. Alerts should be set up for false attempts of logging into your accounts. Two-factor authentication should be set up for your private accounts. Services that do not require mobile phone numbers should be provided with the phone numbers. There are also some authentication apps present such as Google Authenticator, Authy etc. that can certainly prove to be helpful. PINs and passcodes provided by the US cell phone providers can also be used to separate your number from your account.


Jason A Williams
@GoingParabolic
The interest I make a year in #Bitcoin is a pro athletes salary. @BlockFi
GIF
11:06 AM · Nov 17, 2020 · Twitter for iPhone

Williams recently **noted**:

> *"I had a huge position in GUSD and I put it all in BlockFi as a test so I did that over a year ago. I took, as a test, $2.5 million in a money market in a bank and then I took $2.5 million cash and bought GUSD, and put it on BlockFi."*

He continued:

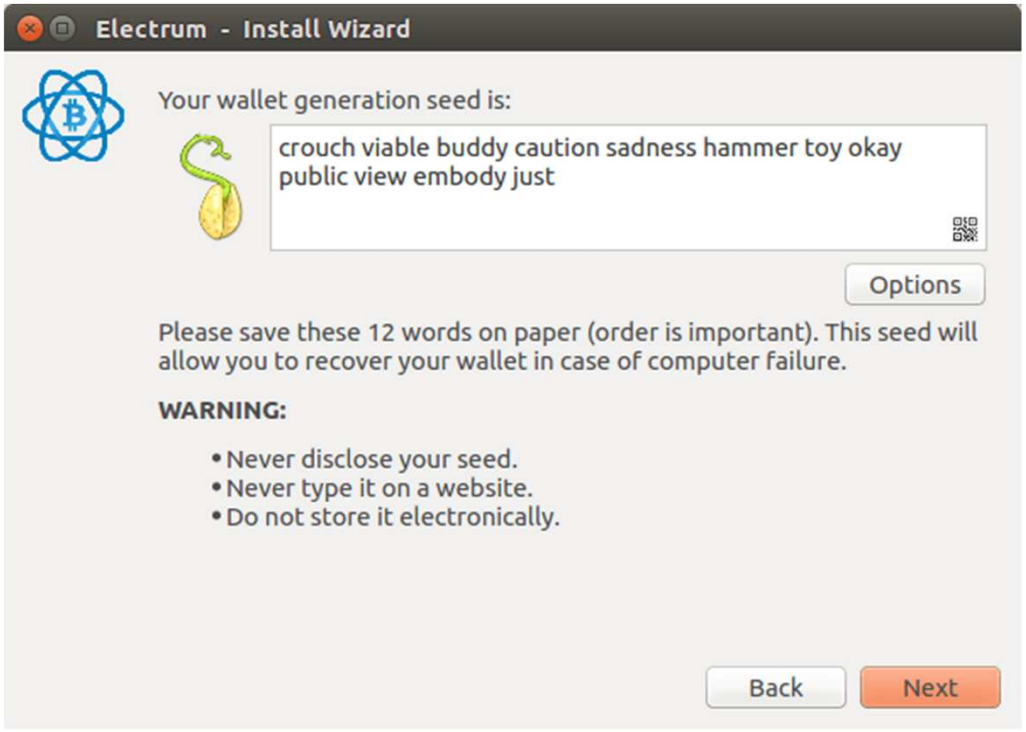
> *"I just held it there and the proof is in the interest…minus fees, minus [all other transaction costs,] I got $5,000 in interest from my money market. I think they were paying me 0.20%. I was getting 8.6% APY on GUSD, so I made $215,000 in GUSD cash via BlockFi."*

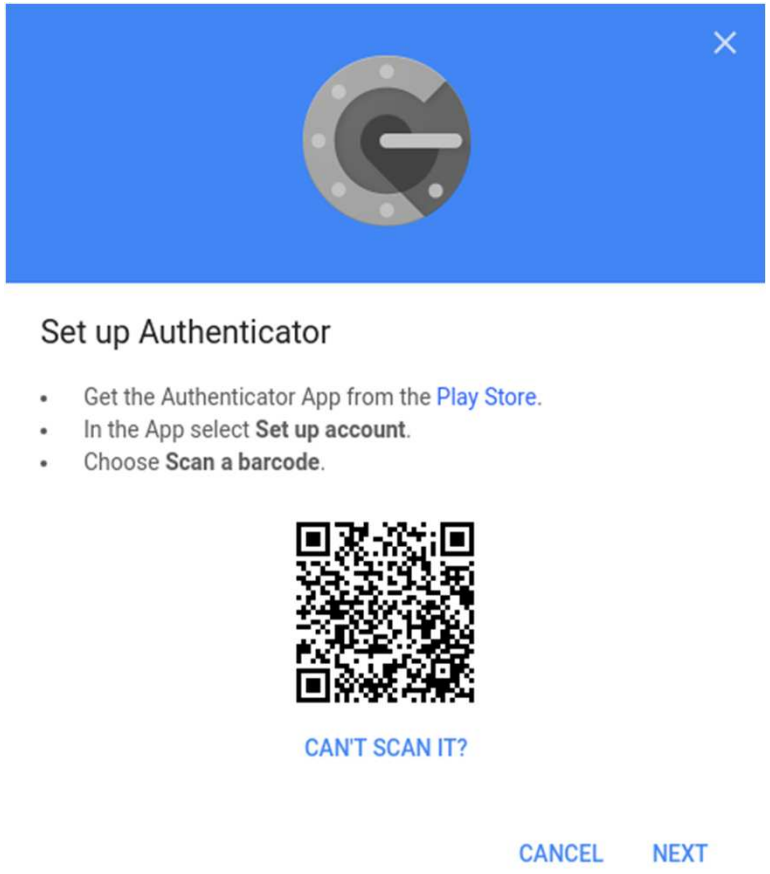
He adds:

> *"It's a no brainer."*

Williams is an angel investor at Duke Angel Network, RTP Capital Associates, Undercover Colors, and several other organizations. He's also an advisor to Innovations in Healthcare at the Duke University School of Medicine.

BlockFi recently appointed Adam Healy as its new Chief Security Officer, which is only a month after the company suffered from a SIM card swap data breach.


Electrum - Install Wizard
Your wallet generation seed is:
crouch viable buddy caution sadness hammer toy okay public view embody just
Options
Please save these 12 words on paper (order is important). This seed will allow you to recover your wallet in case of computer failure.
WARNING:
• Never disclose your seed.
• Never type it on a website.
• Do not store it electronically.
Back
Next


Set up Authenticator
Get the Authenticator App from the Play Store.
In the App select Set up account.
Choose Scan a barcode.
CAN'T SCAN IT?
CANCEL
NEXT


Jason A. Williams "Parabolic Guy"
@GoingParabolic
The smartest people I know reserve the right to change their mind. They even do it on occasion.
9:00 AM · Feb 27, 2021 · Twitter for iPhone
82 Retweets 8 Quote Tweets 1,018 Likes


Jason A. Williams 🚀 @GoingParabolic · May 15, 2017
The consequences associated with the breakthrough of building a Blockchain Electronic Medical Record are hard to overstate @APompliano
GT3RS
5

ATT-WIL-02202


Jason A. Williams 🚀 @GoingParabolic · Jul 17, 2018
Replying to @Crypto_Grit and @Bleeding_Crypto
My lambo for realz. I'm going bigger if bitcoin goes 25k by year end. What should I get?
15
17


Jason A. Williams @GoingParabolic · Apr 15, 2018
Replying to @landoncassill and @Yates_Doug
Just come over and pick one 1000's of horses over here.
1
1
7


Jason A. Williams @GoingParabolic · Mar 14, 2018
Replying to @cindypinkceo
That is so cool. Had a similar thing happen today to me. When you drive to your new start up and your old startup retargets you in an ad.
AT&T LTE
9:49 AM
51%
4.0 miles to I-540 W
Creedmoor Road 6500, Raleigh
OPEN
FastMed - Creedmoor
Flu Prevention, Testing & Treatment - No Appt Necessary!
DRIVE THERE
Adds 9 mins
MPH
Falls of Neuse Rd
Townfield Dr
Spruce Tree Way
14 min
10:04
9.7 mi.
1
1
3

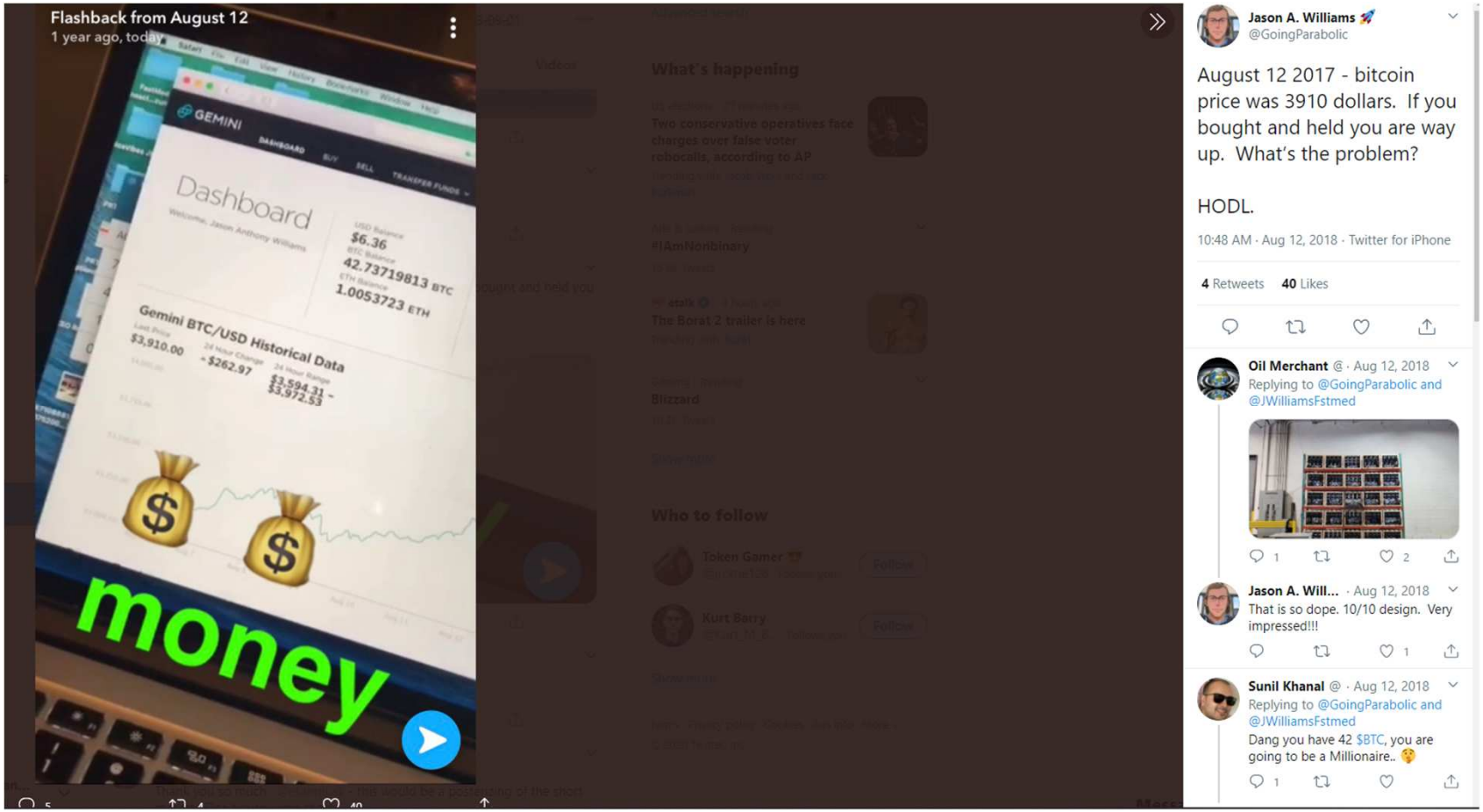

Jason A. Williams 🚀 @GoingParabolic · Jan 4, 2018
Replying to @mhafez @madhu_ and @APompliano
Gemini for direct link to bank. Buy Ethereum and Bitcoin here. FDIC ensured cash and bond to back up crypto. Polo and Binance for Altcoins.
2

Jason A. Williams 🚀 @GoingParabolic · Aug 16, 2018

Replying to @7XFWA @APompliano and 4 others

I like Binance and Gemini. I have had pretty good experiences with them. I think coinbase could be the crypto google.

1 6


Flashback from August 12
1 year ago, today
GEMINI
Dashboard
$6.36
42.73719813 BTC
1.0053723 ETH
Gemini BTC/USD Historical Data
$3,910.00
-$262.97
money
What's happening
Two conservative operatives face charges over false voter robocalls, according to AP
#IAmNonbinary
The Borat 2 trailer is here
Blizzard
Who to follow
Token Gamer
Kurt Barry
Jason A. Williams
@GoingParabolic
August 12 2017 - bitcoin price was 3910 dollars. If you bought and held you are way up. What's the problem?
HODL.
10:48 AM · Aug 12, 2018 · Twitter for iPhone
4 Retweets 40 Likes
Oil Merchant @ · Aug 12, 2018
Replying to @GoingParabolic and @JWilliamsFstmed
Jason A. Will... · Aug 12, 2018
That is so dope. 10/10 design. Very impressed!!!
Sunil Khanal @ · Aug 12, 2018
Replying to @GoingParabolic and @JWilliamsFstmed
Dang you have 42 $BTC, you are going to be a Millionaire..

Jason A. Williams 🚀 @GoingParabolic · May 31, 2018

Replying to @thedr00 @APompliano and @MarkYusko

If you lost the private key on Bitcoin Blockchain than in theory you would not be able to transfer the asset. Just as if you lost the private key to your wallet and didn't have the restore phrases.

1

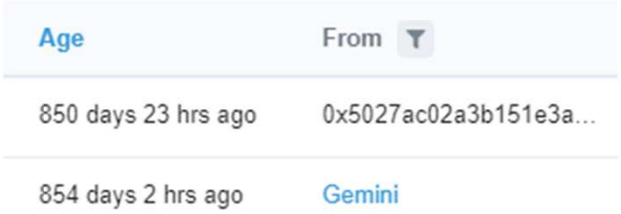
Jason A. Williams 🚀
@GoingParabolic

Replying to @cjking711

Really. Crap I just changed my name from Jason Williams to 0x5027ac02a3b151e3ac41f9bb864feb14606af1b7

11:42 AM · May 31, 2018 · Twitter for iPhone

9 Likes



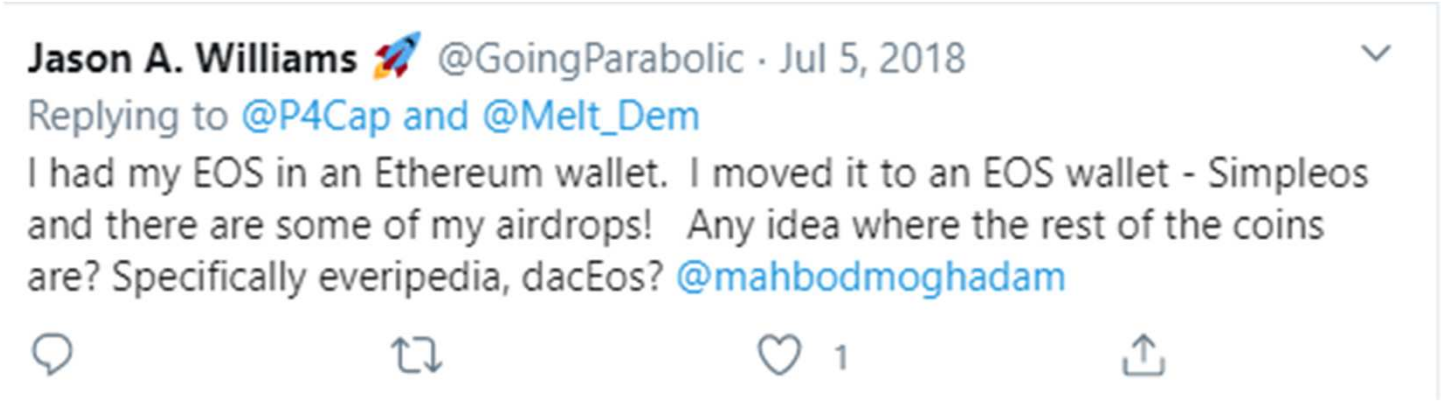
Age	From
850 days 23 hrs ago	0x5027ac02a3b151e3a...
854 days 2 hrs ago	Gemini

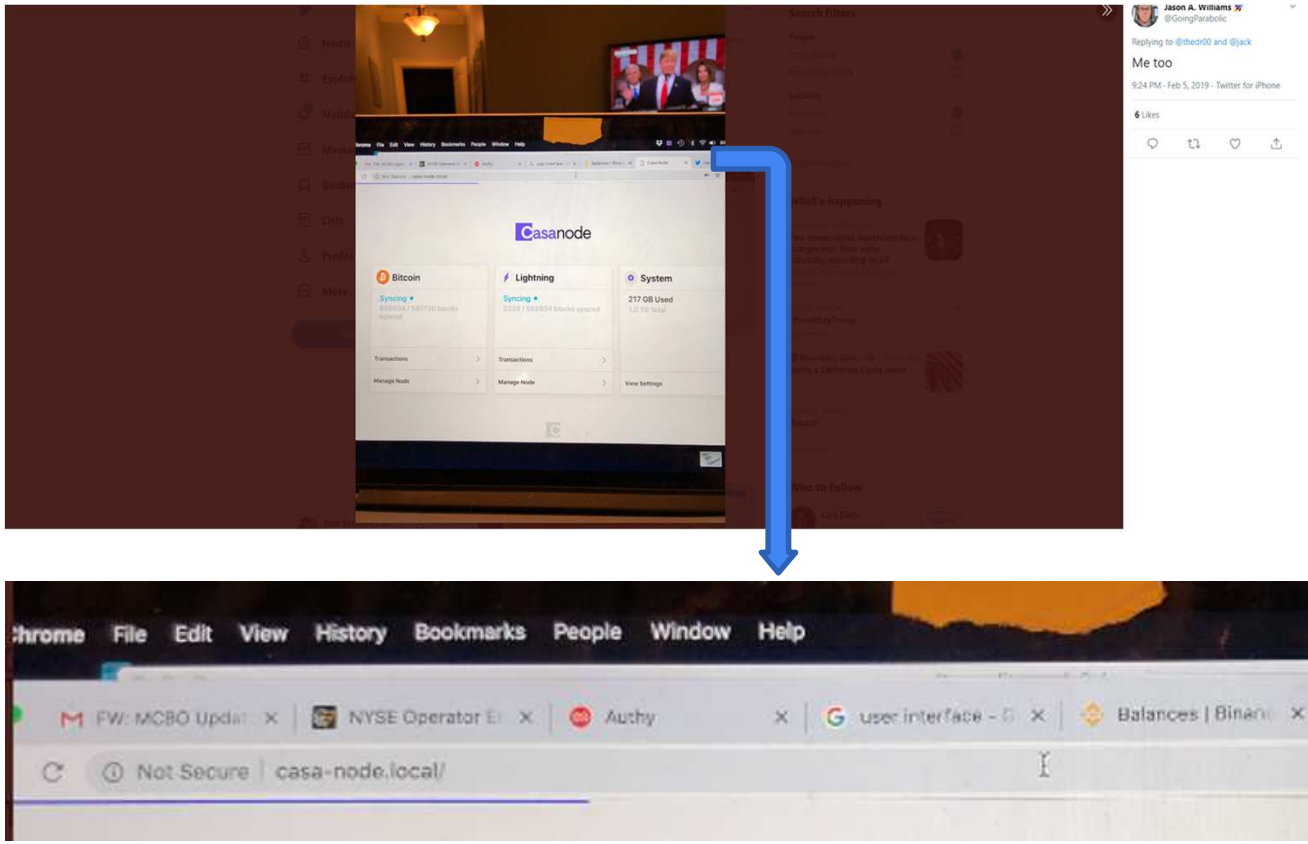
Jason A. Williams 🚀 @GoingParabolic · Apr 28, 2018

Replying to @lowerjd

Not at all. I have no relationship with Binance other than having an account (trading myself).

1


Jason A. Williams 🚀 @GoingParabolic · Jul 5, 2018
Replying to @P4Cap and @MeIt_Dem
I had my EOS in an Ethereum wallet. I moved it to an EOS wallet - Simpleos and there are some of my airdrops! Any idea where the rest of the coins are? Specifically everipedia, dacEos? @mahbodmoghadam
1


Jason A. Williams
@GoingParabolic
Replying to @thedri00 and @jack
Me too
9:24 PM - Feb 5, 2019 - Twitter for iPhone
6 Likes
Casanode
Bitcoin
Lightning
System
217 GB Used
Chrome File Edit View History Bookmarks People Window Help
93
FW: MCBO Upda
NYSE Operator E
Authy
user interface - S
Balances | Binan
Casa Node
Jason A. W
Not Secure
casa-node.local/


Jason A. Williams "Parabolic Guy" @GoingParabolic · Aug 1, 2018
Slushpool just announced zero fee mining 😳😳😳
Until the end of September you can mine Zcash and receive 100 percent of mines coins.
The proverbial "Hash Grab"
1
16
Alexander The Hodler @AlexLary1 · Aug 1, 2018
yeah bitcoin.com is zero to! LMK if slush gets you more. do they share the transaction fee?
1
1
Jason A. Williams "Parabolic Guy"
@GoingParabolic
Replying to @AlexLary1
I already mine on slush.
1:52 PM · Aug 1, 2018 · Twitter for iPhone
1 Like

EXHIBIT C

Keep Your Slush Pool Account Safe

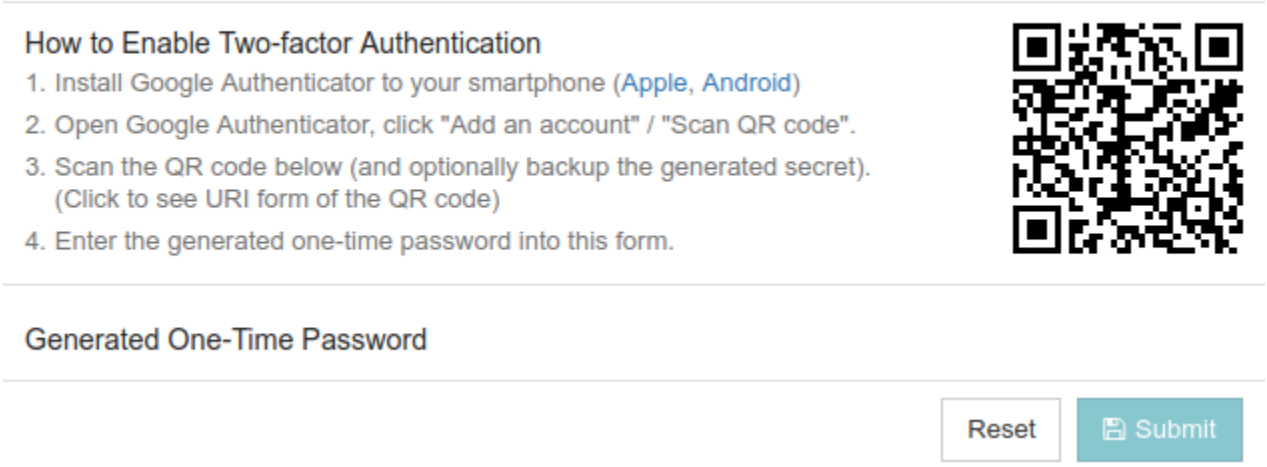
Slush Pool Follow
Sep 27, 2017 · 3 min read

> *Internet security is a very complex field. However, sometimes you can achieve fairly high level of security with quite a **low effort**. It is no different on Slush Pool. Please take a few minutes to read this article and make sure your Slush Pool account is adequately protected.*

Activate Two-factor Authentication

You probably know this. Two-factor authentication can be set up (Settings → Security) using the apps like Google Authenticator or Authy. The app generate security codes that changes over time. In order to login to your account or change some important settings, you have to know **both password and the security code**.

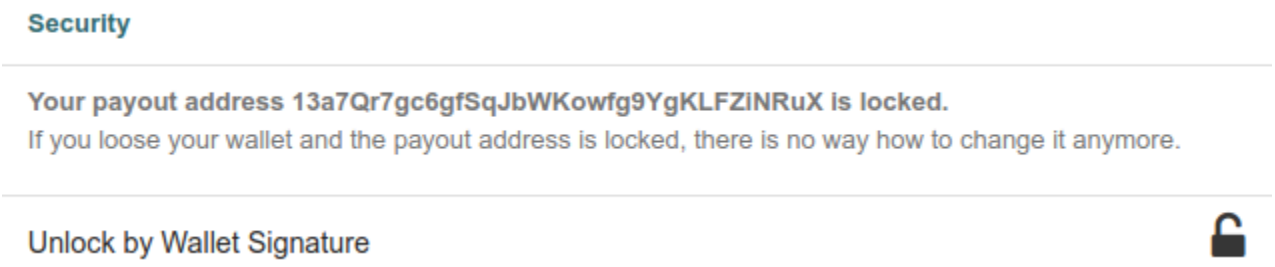
Two-factor Authentication



We also support more advanced (and secure) standard called Universal 2nd Factor. Chances are you already got the TREZOR or a hardware security token like YubiKey so you can use one of those. It is also pretty convenient since you do not have to input security codes over and over again.

Set & Lock Your Payout Address

Firstly, do not forget to set up your payout address. Secondly, consider locking it (Settings → selected coin → Payouts). This is really straightforward and powerful feature. Even if the attacker hijacks your account and bypasess different security measures including 2FA, he **cannot change the payout address** and steal your rewards, as long as he has no control of the specified address.



How it works? If you choose to lock the payout address, you *(or anybody else)* will not be able to select a new address unless you prove that you **control the current one**. That is done simply by signing given text with the corresponding private key. **Be careful** though, this feature is kinda like a *double-edged sword*. You cannot unlock the payout address if you lose the private key or if your wallet does not support signing messages!

Read The Emails

Seriously. We do not like spam and we usually reach you only when **something important** is going on with your account. Unfortunately, a lot of miners do not read the messages at all or (worse) just open them and blindly click the confirmation button. This is an easy way to lose control over your account and *let the bad guy in*.

Also — do not rely solely on timing of those confirmation emails. The attacker could utilize some kind of social engineering to trick you into confirming what he wants. Always check the important details like new payout address etc.

Stay safe and Mine As One!

Security Bitcoin Mining

INDUSTRY | PRODUCT | TECHNICAL

Jan 26, 2017

Better Two-Factor Authentication (2FA)

We have required all of our customers to use two-factor authentication (2FA) from day one. In keeping with our security-first philosophy of protecting and educating our customers, we want to provide some background on our 2FA system ***to encourage our customers to use the Authy app for 2FA rather than SMS***, and to dispel some common misconceptions.

About Authy

Gemini uses the Authy service for 2FA. Authy is an independent cloud service called on to perform secondary verification once we have checked that a customer has provided correct login credentials (i.e., email and password).

Authy offers multiple options for second-factor verification:

automated text-to-speech system.

3. **Mobile application**: Users install an app (or Chrome extension), which generates an OTP based on a secret "seed" and current time according to the TOTP standard. TOTP is an open standard implemented by multiple apps including Google Authenticator and the Authy app.

4. **OneTouch**: Pioneered by Duo Push, this model dispenses with codes altogether. Instead users confirm a login by responding to a simple yes/no prompt.

Each of these options comes with different tradeoffs. **SMS** is simple and can work on any mobile phone including legacy flip-phones that are not "smart" and don't have an application ecosystem. **Voice** codes further improve accessibility by allowing codes to be sent to landlines or heard by users who have difficulty with visual information.

TOTP codes generated using an app do not require internet connectivity. TOTP apps can work offline, even if the phone itself has no service (e.g., when a user is outside a service area). **OneTouch** further improves usability by avoiding the need to transcribe digits from one device to another, but (unlike TOTP) it does require a data connection.

Encouraging Mobile Apps

Gemini has always supported SMS and mobile app options for 2FA. However, in recent interactions with customers, the Gemini support team reached the conclusion that many customers were either not aware of the Authy mobile app, incorrectly viewed SMS as equivalently secure to the Authy app, or were interested in other

for nearly all customers, as discussed below.

At the same time, we recognize there is no one-size-fits-all solution. Customers may have unique requirements which rule out the Authy mobile app, so we will continue to support SMS. However, once you have Authy installed, you will no longer be able to request codes via SMS. We're doing this to prevent would-be attackers from circumventing the security of the Authy app by falling back to SMS.

Risks Associated with SMS

A 2003 ruling by the Federal Trade Commission (FTC) called for number portability between wireless carriers, which allows consumers to keep their existing phone number when they switch from one wireless carrier to another wireless carrier. Number portability increased competition between wireless carriers by removing one of the major obstacles that prevents consumers from switching to a better plan: the hassle of losing their existing phone number. The FTC ruling made it much easier for consumers to keep their number while switching carriers—too easy, perhaps. Call it the law of unintended consequences: the drive to portability also inadvertently opened the door to number-porting attacks.

Last July, the National Institute of Standards and Technology (NIST) came out with a recommendation to deprecate the use of SMS for 2FA. Almost on cue, the industry experienced an uptick in the incidence of phone number hijacking events. In this type of fraud, a miscreant impersonates the legitimate customer and ports his or her number to a *different* carrier, pretending to be that person switching carriers. If the attacker is successful in convincing the other carrier to reassign the number to an attacker-controlled device, all voice calls and SMS messages will be routed to the perpetrator. As a result, *any*

Setting up the Authy Mobile App

Setting up the Authy mobile app eliminates the risks associated with using SMS for 2FA, however, to fully mitigate SMS vulnerabilities ***you need to make sure you turn off "multi-device" in the Authy app.*** This prevents the same number-porting attack (mentioned above) from being used to obtain access to your SMS messages to perform an unauthorized install of your Authy account. When it is turned off, no additional instances of the Authy app can be provisioned. We recommend all Gemini customers to keep multi-device disabled, only enabling it ***temporarily*** when setting up a new device (for example, when upgrading your phone). If you're resetting or trading in your phone, we also recommend that you install the Authy desktop app first, so that you can use it to authorize your new phone. We are also working with the Authy team to make the process of switching or upgrading devices easier and more secure for all Gemini customers, regardless of your multi-device settings.

Looking Forward

While using a mobile app to generate codes is an improvement, there are other attack vectors that no 2FA solution based on one-time passcodes (OTPs) can solve. For example, sophisticated phishing attacks can ask users to disclose *both* their password and an OTP code. This type of phishing is more complex because it requires real-time use of compromised credentials. Since OTPs expire after a short time period, it is not possible to stash the stolen credentials for later use. Despite that added complexity, such attacks are not only feasible in principle but they have been observed in the wild against popular 2FA implementations including those used by Google and some large financial services companies.

website, phishing remains a viable attack. For these reasons, ***we are continuing to explore alternative 2FA paradigms such as U2F or Authy OneTouch for Gemini*** which are based on fundamentally different models. (Case in point: our *internal* systems for administering the exchange use public-key authentication with hardware tokens based on the PIV standard.) Our priority is to find a solution that combines high security and usability, and is available to our customers across a broad range of platforms.

Cem Paya

Security Team

Similar Articles

INDUSTRY

Twitter Roundup: April 16, 2021

Apr 16, 2021 | Team Gemini

INDUSTRY

Twitter Roundup: April 9, 2021

Apr 09, 2021 | Team Gemini

INDUSTRY | PRODUCT

Gemini Builds Out UK Institutional Offering

Apr 07, 2021 | Blair Halliday

INDUSTRY

Gemini To Custody BTG Pactual Bitcoin Fund

Apr 05, 2021 | Team Gemini

INDUSTRY

Twitter Roundup: April 2, 2021

Apr 02, 2021 | Team Gemini

GEMINI

Get started

Get Started

Create a free Gemini account in minutes

Register

For Institutions

Check out our portfolio of client solutions

Learn More

GEMINI

Buy and sell bitcoin, ether,
and other cryptocurrency.

Stay up to date

Enter your email address below.

Submit

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

GEMINI

Get started

Gemini ActiveTrader™
Gemini Clearing™
Gemini Custody™
Gemini Wallet™
Gemini dollar™
Gemini Earn
View All

Brave
Nifty Gateway™
Affiliate Program
View All

Security

Institutions

Company

About Us
Blog
Newsroom
Careers
FAQ
Email Us
Help Desk
Status

Resources

Prices
Cryptopedia
Videos
API Docs
Refer a Friend
Auction Data
Marketplace & Fees
Areas of Availability
Legal Agreements

Get the app

Download on the App Store
GET IT ON Google Play
Available on Galaxy Store

GEMINI

Get started

How to increase your Coinbase account security

soupsranjan Follow
Apr 22, 2017 · 6 min read

We advise our users to install Authenticator apps (Google Authenticator, Microsoft Authenticator) as their primary 2FA method to secure their Coinbase accounts from phone porting attacks. You can follow the steps outlined in our support article to use Authenticator.

The instant and irreversible nature of digital currency enables fascinating use cases and drives our mission to create an open financial system for the world. This includes helping merchants accept bitcoin with no chargeback risk and helping users do global remittances instantly at low fees. But that very nature of bitcoin also attracts sophisticated attackers that challenge this mission.

Security of any system is as strong as its weakest link. Recent attempts to break into Coinbase user accounts point back to that weakest link being telecom companies (telcos). I'll explain that after a brief overview of two factor authentication.

Two-Factor Authentication (2FA):

When you log in to any service in the cloud that's storing anything of value (money, data, assets) it is crucial to have two factors. The first is something you *know* (a strong password) and the second is something you always *have* (like your mobile phone). Sending a 6 digit pin code via SMS to your mobile phone, allowed online services to verify during the login process that it was indeed you who requested access to the service.

It was intended for the second factor to be the physical device that you always have in your control. But, sending SMS to your phone actually verifies you have access to your

phone number, not really your phone device. This distinction is really important as it turns out phone numbers can be stolen far more easily than physical phone devices.

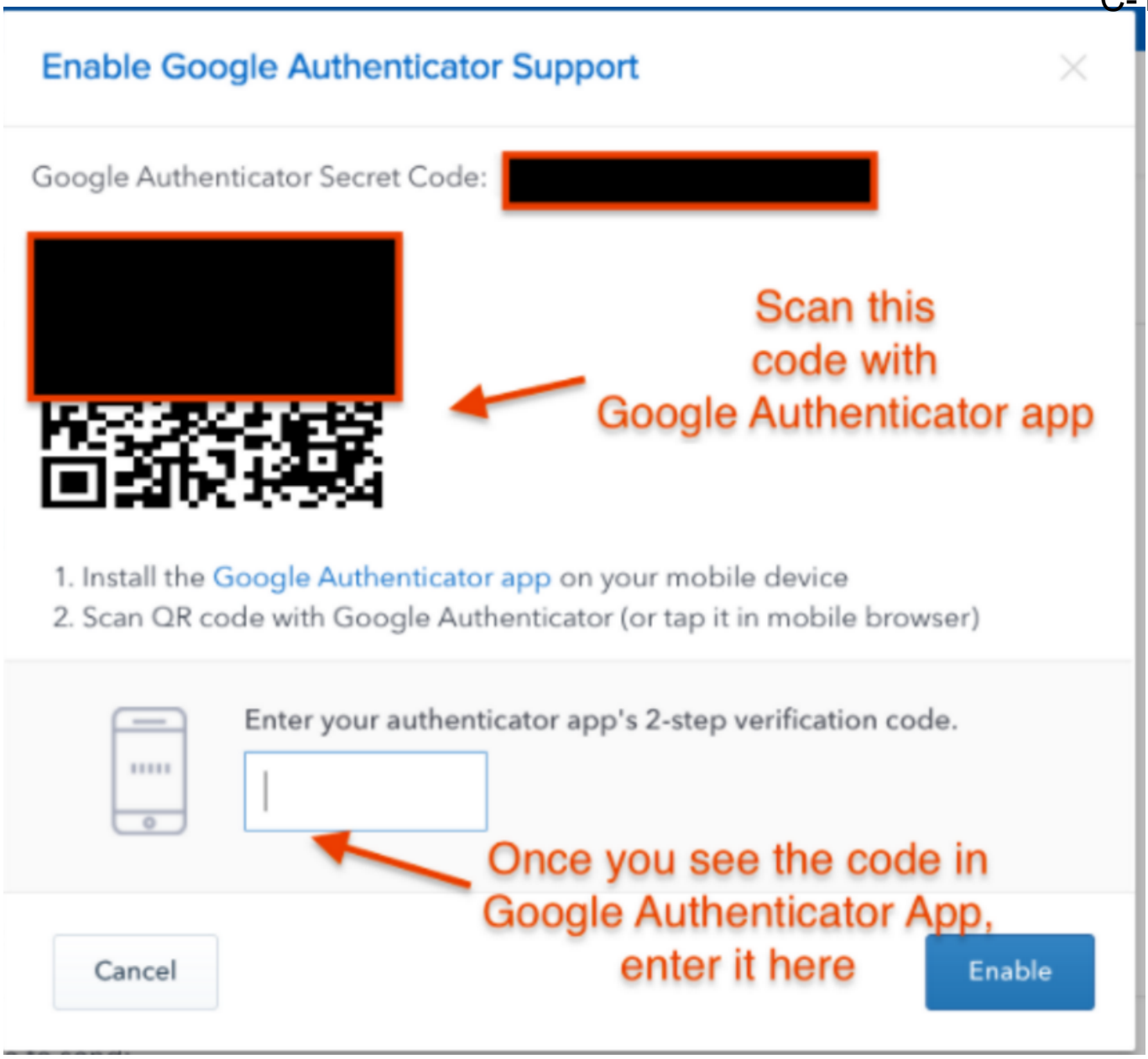
Telcos as weakest link in SMS based 2FA

Telcos break the assumption that SMS based 2FA is reliable for two reasons. First, some telcos allow SMS to be readable online thereby making SMS based second factor only as strong as user's telco billing password. Secondly, poor security processes at telcos around phone portability enable attackers to takeover accounts more easily. In the past several months, we've been working behind the scenes to stay ahead of these attacks. We wrote about this recently and would like to share things we have since built to keep our users safe despite these vulnerabilities. In a second blog post, I will provide more details of the vulnerabilities exposed by poor security practices at telcos.

Authenticator as your primary second factor authentication:

We recommend all users, especially those with high balances or those more security conscious to install device-only 2FA apps which are also commonly referred to as Authenticator apps, examples being: Google Authenticator, Microsoft Authenticator, etc.

You have to first download the Authenticator app on your mobile device and then you would scan a QR code on Coinbase's security settings page. This QR code is essentially a secret key that is shared securely *once* between your mobile device and Coinbase. The Time-based One Time Password (TOTP) protocol is then used to authenticate you every time you try to log in to Coinbase. Next time you log in to Coinbase and use your Authenticator app, the app will use the current time of day and the secret key to generate a 6 digit code. When you enter that 6 digit code on Coinbase, we'll check if it is valid by using the same parameters (current time of day and the secret key). You will notice that with this 2FA method, no data is ever shared over the air unlike SMS. Hence, it is much more secure to man-in-the-middle attacks.



How to enable Google Authenticator as primary 2FA on your Coinbase account

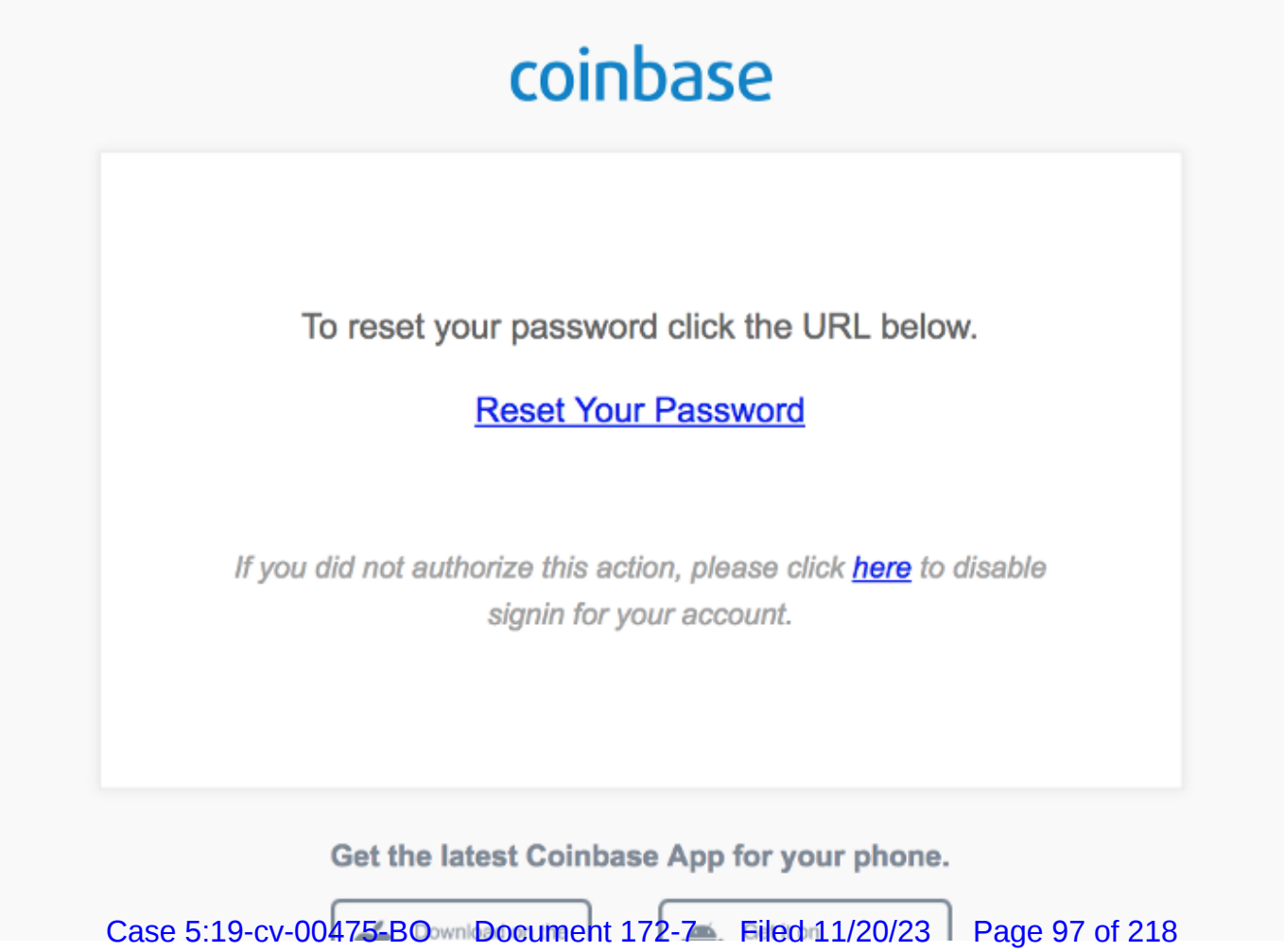
For making future account recovery easy, we recommend users should note down the *secret key* that is generated after linking Coinbase with their Authenticator app on a piece of paper or a USB key that should be kept offline. In a forthcoming release, we will have backup recovery codes and then we'd recommend you to write those down instead. Note that you are trading-off usability for security with this choice. So if you lose the device where you've installed the Authenticator app and do not have access to your secret key, then you'll have to contact Coinbase support. This is why it is important to write down the secret key and store it securely at the time of setting up Authenticator to avoid delays in account recovery later on.

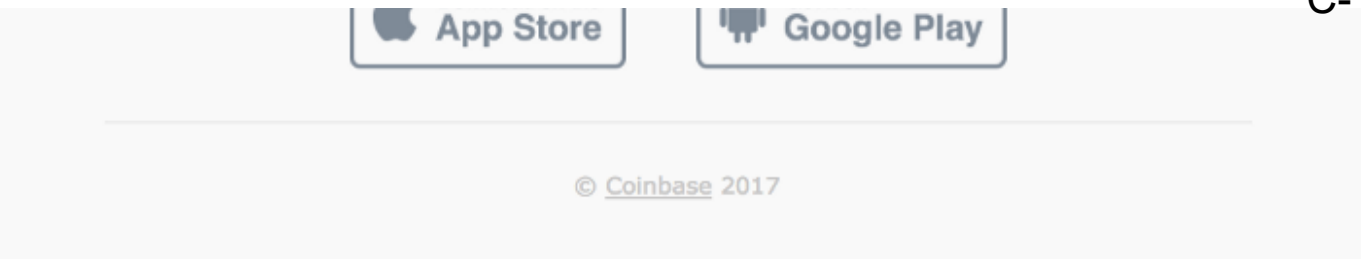
We also support the use of Authy app, which instead of using the traditional QR code method to send you your secret key, uses an API to deliver the secret key securely to your device. Once you've installed Authy, we recommend disabling the *Multi-device* option. This means nobody can add a new Authy app to your account. Also pay attention to any emails or SMS messages you may get from Authy as they may communicate with you if they see someone trying to change your 2FA data.

Auto Lock your account on seeing suspicious activity:

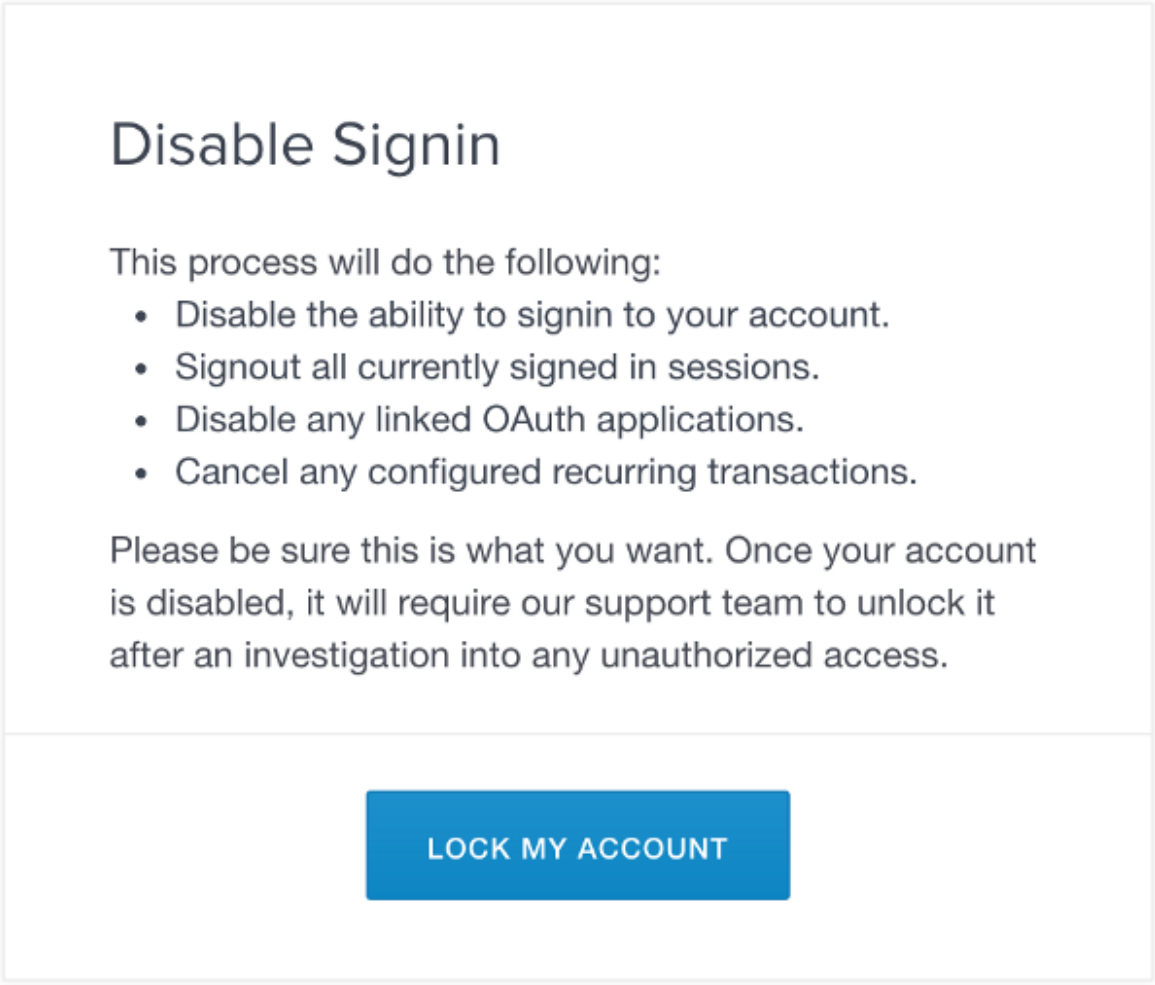
Please pay special attention to SMS or emails from Coinbase that inform you that your 2FA settings or password have been changed or a new device has been added, or a withdrawal has been made from your account.

You can also **auto lock** your account by following a special one-time use link that we recently added at the bottom of our emails. That link leads you to a Disable Signin page. When in doubt, always hover over any URL link to first confirm it leads you to Coinbase.com before clicking it.





Our security sensitive emails have a special link you can click on to lock your account



You can lock your account when you suspect unauthorized access

Balancing security with usability:

Balancing security with usability is always a hard product trade-off. We balance this trade-off by making our second-factor authentication an opt-in. So users who want to continue using SMS based second-factor authentication, can still do so. We can't move them over to Authenticator overnight without a significant amount of hand-holding. In

light of this and despite vulnerabilities in SMS-2FA, we still need to protect those users' funds from account takeovers. We are actively working on an account takeover detection system that uses behavioral anomaly detection and will delay withdrawals of digital currency from suspicious sessions. We expect to launch this feature within the next few months. Stay tuned.

In a lot of respects, Coinbase is building one of the most sophisticated security companies in the world. We use advanced cryptography, state-of-art 2FA, data science and machine learning to stay one step ahead of the attackers. If you'd like to join us in our mission to help make finance 2.0 user friendly as well as secure, please look at https://www.coinbase.com/careers.

I'll also be presenting on this topic and risk engineering in general at the following venues. Come check them out:

- Data Eng Conf, SF, Apr 28
- Risk Salon's Deflect Conference, SF, May 18
- QCon, New York, June 26–28

Thanks to my colleagues: Tom Boice, Linda Xie, Dave Farmer, Rob Witoff and Jeremy Henrickson for reading multiple drafts of this article and risk- and security-engineering teams at Coinbase for pushing the bar on security at Coinbase.

Updated: on Apr 25 with minor edits to clarify that Coinbase supports all Authenticator apps (Google Authenticator, Microsoft Authenticator, etc)

Startups Security Tech Ethereum Bitcoin


Download on the
App Store


GET IT ON
Google Play

MOTHERBOARD
TECH BY VICE

How to Protect Yourself From SIM Swapping Hacks

Here's a guide on how to prevent and protect yourself against the threat of hackers taking over your phone number and going after your online accounts.

By Lorenzo Franceschi-Bicchierai

July 17, 2018, 9:32am

How to Protect Yourself From SIM Swapping Hacks

Criminal hackers have been targeting Instagram users with short or unique usernames, as well as people who own Bitcoin. To steal the victim's accounts or cryptocurrencies, the hackers first seize the cell phone numbers of targets, which gives them the ability to reset passwords on any account linked to a given number.

This kind of hack is what's called a port out scam—an expression derived from the concept of porting a number from one carrier to another—and is also known as SIM swapping or hijacking. One hacker who used to SIM swap told me it happens "all the time," despite telecom providers having known about this attack method for years. According to T-Mobile, hundreds of people have been hit by this scam. In the last few months, Motherboard has spoken to more than 30 victims who have gotten their numbers stolen. In addition to her Instagram handle, one SIM hijacking victim I spoke to got her Amazon, Ebay, Paypal, Netflix, and Hulu accounts hacked as a result.

"Our phones are our greatest vulnerability," she told me.

> ***Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzo@jabber.ccc.de, or email lorenzo@motherboard.tv***

So, what can you do to protect yourself?

Ultimately, this hack relies on scammers tricking carrier's tech support, and if the company's representatives take the bait, it's important to remember that there's only so much you can do. The good news is you can make it considerably harder for hackers to steal your phone number. And, even more importantly, you can take steps to mitigate the damage in case they are able to steal it anyway.

Here's how.

HARDEN YOUR ACCOUNT

In light of increasing attacks against customer's accounts, the major US cell phone providers have introduced new security features to make it harder for hackers to take over accounts and telephone numbers.

AT&T allows customers to add a passcode to their accounts. This is a credential that's separate from the password customers use to log into their accounts online. This passcode will be required to make significant changes to the account, such as porting the number to a different SIM card. Here's a detailed step-by-step from AT&T on how to turn on this feature.

Verizon says it now requires every customer to have a PIN or password as a "primary authentication" method when they reach out to a call center. This PIN is similar to the passcode that AT&T customers can set up, as it's used when communicating with Verizon tech support and provides an extra layer of security.

Last year, T-Mobile started offering a "port validation feature" to protect against these hacks. This is essentially a passcode, separate from the usual password to access the online account, that is required whenever someone tries to make changes to the account, such as getting a new SIM card. Ask a T-Mobile representative to add this code to your account. This can protect you from a hacker who may pretend to be you on the phone, or from a scammer attempting to use a fake ID at a T-Mobile store, as they should still be required to provide the code.

Sprint also offers customers a separate PIN that needs to provided when doing a SIM swap, in addition to the option of answering a security question instead.

We advise calling your provider directly and telling them that you're worried about criminals taking over your phone number, and asking for all the extra security measures you can take to protect your account.

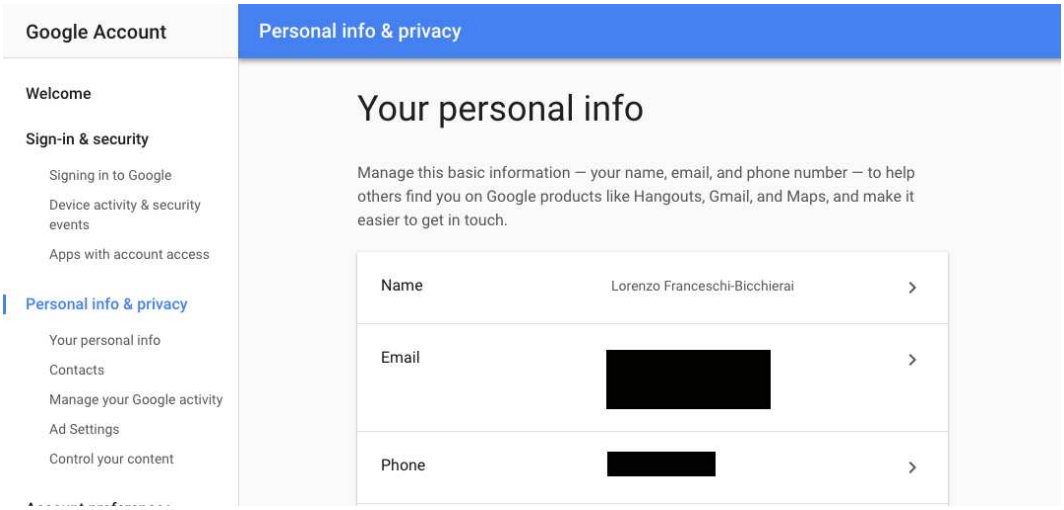
DON'T LINK YOUR NUMBER TO YOUR ONLINE ACCOUNTS

Once hackers steal your phone number, they leverage it to reset the password on any online account that's linked to the number. In many cases, this bypasses two-factor authentication. That's why having control of a phone number is so powerful.

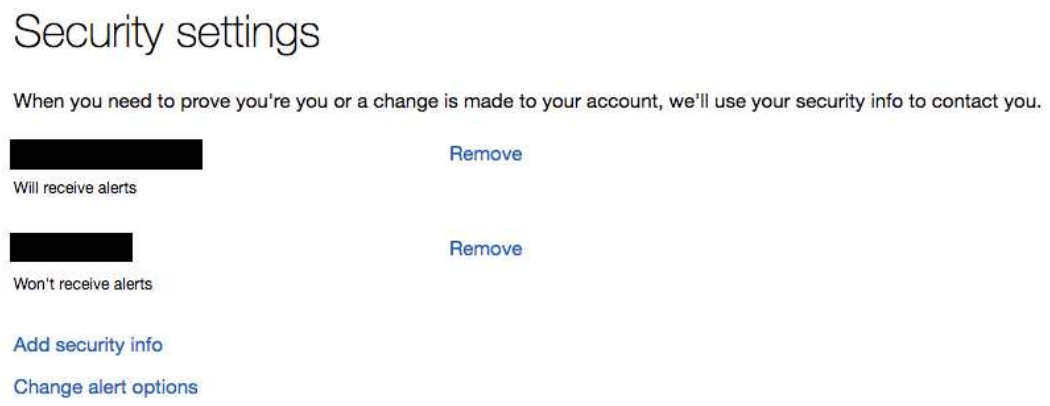
If possible, you should remove your phone number from any account that could interest hackers. You can still link a type of phone number to those accounts, but we suggest using a VoIP number, such as a Google Voice number, that is SIM hijack-proof. Of course, you must protect this number as well, using a unique password, two-factor authentication on the account, and making sure it doesn't expire if you don't use it regularly.

To remove your phone from your Gmail account, go to myaccount.google.com, log in (if necessary), and then click on Personal Info & Privacy and Personal Info. If you have your number there, remove it. Also be sure you don't have a phone number listed under Account Recovery Options. Instead, add an authentication app like Google Authenticator as two-factor.

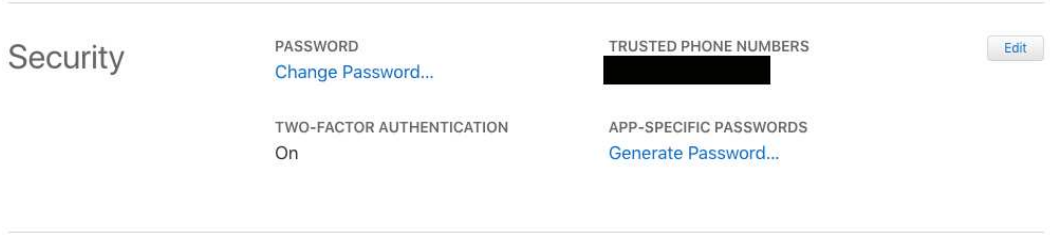
If you really want to have a number there, we suggest creating a new Google Voice number—from a different, ideally ad hoc Gmail account—and use that number. Note that Google Voice is only available in the United States, so anywhere else and you will have to try a different VoIP service. (Pro tip: always create and save recovery codes when you turn on two-factor.)



To remove your phone from your Microsoft account, go to account.live.com, navigate to Security, and then click on Update Info under Update Your Security Info. If you have a phone number there, remove it, unless it's a Google Voice or another VoIP number.

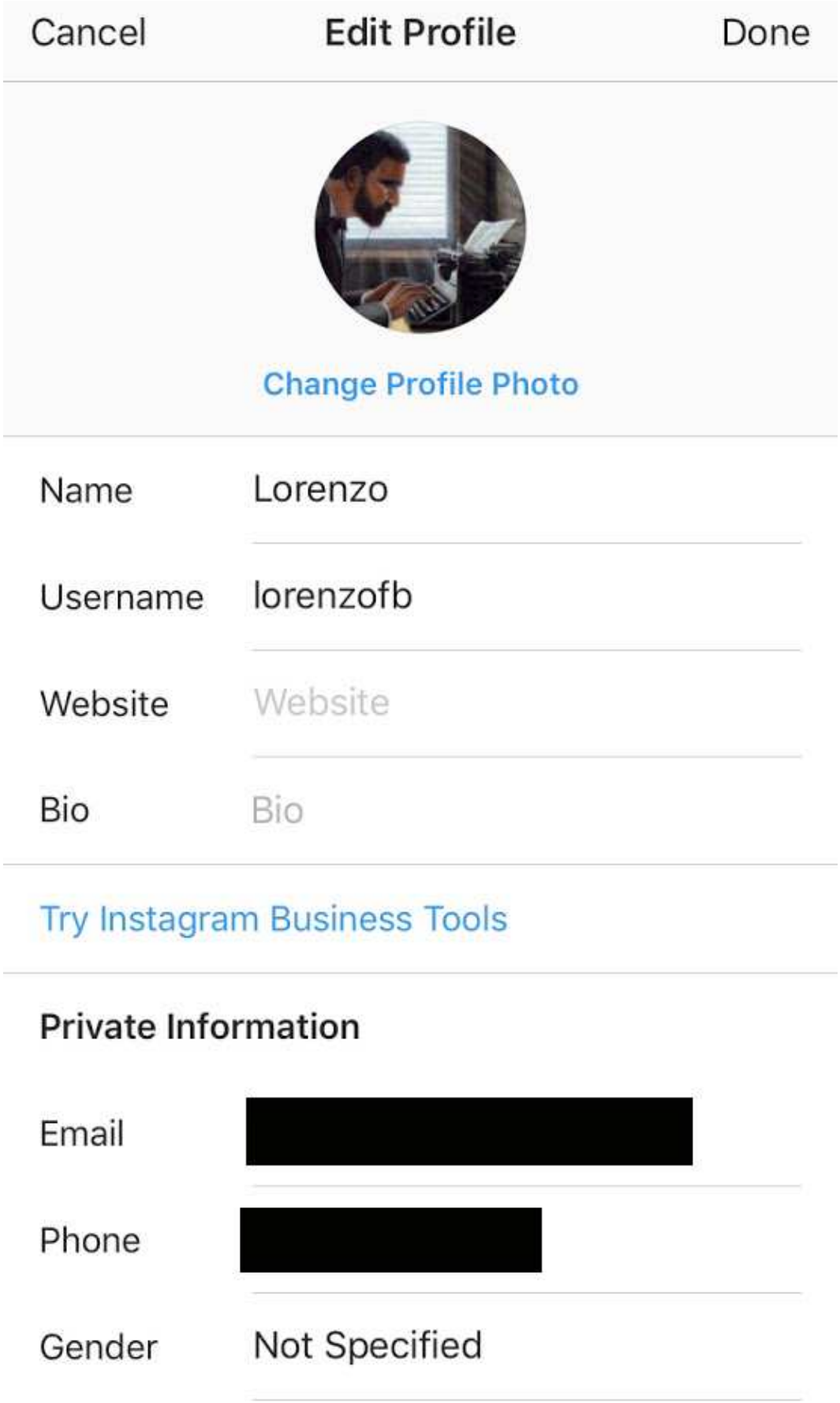


If you use an Apple device, go to appleid.apple.com, log in, then click on Edit next to the Security section. Add your Google Voice or VoIP number as Trusted Phone Number and then remove your regular phone number if you had it there. For iMessage and FaceTime you'll still need to provide your actual cell phone number, but you can use a different one as a Trusted Phone Number.



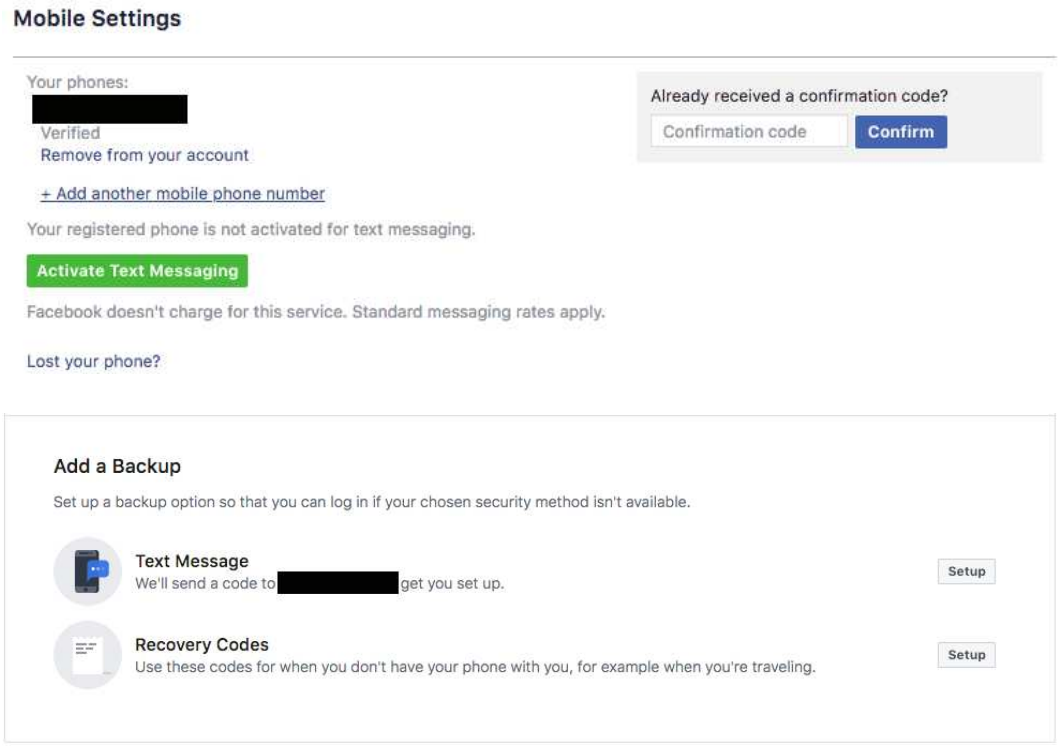
On Twitter, click your avatar, go to Settings and Privacy, and navigate to Mobile on the right hand menu. If you have two-factor enabled, you'll need to provide a number. For this reason, we suggest you provide a VoIP or Google Voice number so that hackers can't SIM swap it. It's also possible to just use an authenticator app or security key and remove your phone number from Twitter altogether.

The situation is similar for Instagram: From the mobile app, click on your avatar, then Edit Profile and change your number to a VoIP or Google Voice number. Unlike Twitter though, it's not possible to remove your phone number altogether from Instagram without turning off two-factor.



For Facebook, select Settings under the drop-down arrow at the top right. First, click on Mobile in the right-side menu, and remove your phone number. Now add

your Google Voice or other VoIP number. Then navigate to Security and Login (also on the right-side menu), click on Edit in the Use Two-Factor Authentication option, and make sure your new VoIP or Google Voice number is there.



Finally, for Amazon, click on Accounts and Lists, then Your Account. Then click on Login & Security, input your password, and check if you have your number listed there. If you do, you know the drill: swap it for your VoIP or Google Voice number.

We suggest you do the same for Paypal, eBay, Netflix, and similar other accounts, plus your bank of choice.

Get six of our favorite Motherboard stories every day by signing up for our newsletter.

SIM Swap Fraud Offers Account Takeover Opportunities for Cybercriminals

BLOG JUNE 8, 2018

Key Takeaways

▪ The term SIM swapping has historically referred to phone number takeover using a variety of different methods. These have included password reuse, social engineering of customer service professionals, and using leaked databases and personal information (such as Social Security numbers (SSNs) to facilitate phone line takeover. More recently, observed online activity suggests that organized operations use insider recruitment at the retail level to perform SIM swaps. Assessment and obtained intelligence suggests that almost all major mobile phone carriers are at risk, and that a user's good security practices are unlikely to stop a targeted attack.

▪ Flashpoint analysts assess with high confidence that the potential impact of SIM swapping is likely high for anyone targeted in such attacks. While Flashpoint has observed extensive targeting of high-

SIM Swap Fraud Offers Account Takeover Opportunities for Cybercriminals

Key Takeaways

• The term SIM swapping has historically referred to phone number takeover using a variety of different methods. These have included password reuse, social engineering of customer service professionals, and using leaked databases and personal information (such as Social Security numbers (SSNs) to facilitate phone line takeover. More recently, observed online activity suggests that organized operations use insider recruitment at the retail level to perform SIM swaps. Assessment and obtained intelligence suggests that almost all major mobile phone carriers are at risk, and that a user's good security practices are unlikely to stop a targeted attack.

• Flashpoint analysts assess with high confidence that the potential impact of SIM swapping is likely high for anyone targeted in such attacks. While Flashpoint has observed extensive targeting of high-profile individuals and owners of unique usernames that confer social status, financial fraud has also been observed, including targeting online wallets such as Paypal and Bitcoin.

• Mitigations for SIM swap fraud largely rely on website owners changing their authentication logic. Since most websites cannot detect a SIM swap, use of phone numbers for password recovery or two-factor authentication (2FA) remains vulnerable to this attack vector, and mitigations initiated by the end user are not entirely effective.

Background

The term SIM swapping has historically referred to phone number takeover using a variety of different methods. These have included password reuse, social engineering of customer service professionals, and using leaked personal information (such as SSNs) to authenticate access to and subsequently modify an account. Historically, gamer communities have used SIM swapping to take over high-profile social media accounts and obtain accounts with OG (original)

usernames. OG usernames are often a signifier that the user registered on a platform early, conferring social status in some online communities. Dictionary words and short usernames are typically highly desirable, so a username of "dog" is considered far more desirable than "dog789;" typically, a single character username is the most desirable. In the past, this activity had only minor financial motivations, but this appears to have shifted.

Over time, people engaged in this activity have amassed a collection of techniques that they use for the targeted takeover of accounts with a high rate of success. Most of these techniques require a security lapse on the victim's part, but some do not.

Insider Recruitment Campaign

Flashpoint analysts observed an insider recruitment campaign mostly targeting employees at mobile phone carriers. In this campaign, threat actors paid insiders a small sum of money in exchange for executing a SIM swap on a targeted customer's account.

In this campaign, attackers took over prominent users' social media accounts and posted recruitment spam. These hijacked accounts had a large number of followers and a high degree of follower engagement, so these posts reached a wide audience before being deleted.

Flashpoint analysts were able to determine that all the affected users had their phone numbers hijacked; attackers used that access to hijack their email addresses and social media accounts, thereby locking the original owners out of the accounts entirely. Some lockouts were remediated with a call to the company's customer service, but some websites were extremely difficult or impossible to recover stolen accounts from. Some victims reportedly gave up trying to regain control of their accounts, so some thefts were effectively permanent.

Anyone responding to the recruitment advertisements would be vetted by the hijacker to ensure that they really are an employee of the company, and that they are willing to abuse their employee access in exchange for money.

One example conversation is below. Flashpoint analysts redacted specific names to protect sources and censored profanity:

Insider: I work at [company name]

Hacker: If so

Hacker: whats [company internal tool name]

Insider: its an application used to look at business and client info why

Hacker: ok what else can u do on it

Insider: Process payments basically the whole business runs off this app

Insider: But it wont be around for much longer so idk why you need to know this

Insider: Do you wanna change rate plans?

Hacker: ok

Hacker: what else

Insider: What do you mean what else lol you wanna do this or not

Hacker: Ok

Hacker: Download an app called telegram

Hacker: So we can talk about money etc on there

Hacker: My username is [redacted]

Hacker: Lmk once u messaged me on it

Insider: Prove to me this is actually you first

*Hacker: Ni**a*

Insider: How would we make money thoug

Hacker: Basically I'll pay u 80$ for u to update sims for me

Hacker: I'll give u a number to lookup

Hacker: And I'll give u my simcard number to put the number on

Hacker: And for each swap

Hacker: I'll pay 80$

Hacker: Via PayPal or bitcoin

Hacker: And which raises the question on weather u work at Corp or retail cause retail can only bypass with last four

Hacker: And Corp can just go straight in the account

Insider: Lets do this im ready

When probed with different insider offers, this threat actor demonstrated knowledge of internal tools belonging to several mobile phone companies.

The Underground Marketplaces

A number of underground marketplaces exist where users can buy and sell stolen accounts. Depending on the attributes of the account, they are sold for different purposes. Accounts with OG usernames are sold simply for the username. Some accounts have a verified checkmark on the platform, and others have a large number of followers. Accounts with a large number of followers can be used to spread spam or malware. Accounts without an OG username but with a valuable status are called “stat” accounts.

One forum that hosts a large amount of this type of activity is Hackforums. While explicit discussion of fraud is generally frowned upon, the fruits of these labors are often sold openly. Despite the forum’s reputation as a beginner-level community, some of the most prolific actors in the account takeover community sell accounts on the Hackforums marketplace.

In this example, one of the highly prolific actors discusses some of the subtleties of the SIM swap problem in response to another actor’s message how to social engineer wireless providers to obtain account access:

They’d have to get into your account first, 2FA is simply another barrier. Even if you do get simswapped or phone forwarded, having 2FA makes the process of someone jacking your account a lot more time consuming. 2FA is never a weakness; having your number as a recovery option is though.

This actor likely speaks from experience. They were taken into custody and their home was searched in 2015 in relation to the previous TalkTalk hack, and their post history shows they never stopped involvement in account takeover. They have hundreds of sales listings for illegitimately obtained accounts, and other threads related to fraudulent activity including compromised accounts from wireless providers and top social media companies. They also demonstrated

interest in speaking to phone company employees, likely to facilitate additional fraud.

Username Market Values

The market values for OG accounts depend on several factors:

• The popularity of the website on which the account is located.

• The length of the username (shorter usernames are typically preferred).

• Whether the username is pronounceable or a dictionary word.

• The measures the seller took to ensure that the buyer does not get banned and that the victim cannot recover the account. For example, if the seller can also include the email address the account was created with, the likelihood of a ban or account recovery is lower.

• If the account has a verified checkmark or a large number of followers.

Accounts are often stolen due to password reuse, not just because of SIM swapping. Most dictionary words will go for prices between $20 and $100, but prices can go higher for very short usernames, or identical usernames sold across multiple social media platforms as a bundle. The prices suggest that most OG usernames would mostly not account for the bribes offered to telco employees. Other types of fraud are more lucrative.

SIM Swaps in Financial Fraud

A number of high profile fraud incidents reported in the media have involved phone number takeover.

On May 18, 2018, cybersecurity journalist Brian Krebs posted an article about a SIM swap incident involving the OG usernames “par” and “p9r,” which belonged to the same victim. The article claims the victim had already performed the recommended security precautions, including a PIN to prevent number port-outs, but this was not sufficient to prevent a determined attacker. Once the attacker seized control of the phone number, they abused the password-reset logic on multiple websites to take over multiple accounts belonging to the victim.

On June 5, 2018, the South African radio show CapeTalk discussed a SIM swap incident where a retired man lost his entire savings due to a SIM swap. The segment did not refer to any phishing or security lapses on the victim’s part. The

show interviewed a forensic investigator who has worked on these cases in South Africa. The investigator stated that these incidents were on the rise, and that these abuses happened at the employee level. The investigator also stated "there is a dishonest element within the cell phone industry", who can facilitate this type of account takeover "without the proper channels being followed." The investigator referred to his experience in SIM swap cases, and said most victims never receive compensation from their bank. He also referred to the cell phone companies as "extremely hard-hearted" about providing assistance to victims.

On Feb. 10, *The Guardian* published an article claiming that attackers repeatedly called a U.K.-based victim's phone company and eventually fooled an employee into performing a SIM swap, which was immediately used to attempt bank account fraud. In this incident, the bank's voice identification caught the fraud before completion. The victim noted that the cell phone company used extremely simple authentication questions that any attacker could likely figure out the answers to.

On April 20, *MyBroadband*, a South African tech news site, detailed an incident where a SIM swap victim not only lost the contents of their entire bank account, but the attacker took out loans in their name. The article stated that several days before the SIM swap, the victim received a phishing email. Notably, the article said this particular phone company offers banks the ability to query their subscribers to determine if a SIM swap has happened recently on a phone number. This event would place a temporary hold on the account. In this case, the victims were initially told by the phone company that their phone was broken, so they apparently did not take action quickly enough against the fraud. In the ensuing legal battle, the bank, the phone company, and the victim claimed the other parties were liable.

On June 7, 2016, the FTC warned about an increasing trend of SIM swap fraud. While most of the blog post spoke about this technique being abused to get new phones which could be resold, it also mentioned that this was also used to bypass two-factor authentication for banks. The author said this type of fraud was a larger problem in Europe than in America at the time, but added the trend was increasing. The FTC also states that "Section 609(e) of the Fair Credit Reporting Act requires that companies provide business records related to identity theft to victims within 30 days of receiving a written request." For any account takeover victim, exercising these rights may help them understand the nature of their attacker.

Impact

Flashpoint analysts assess with high confidence that the potential impact of SIM swapping is likely high for anyone targeted in such attacks. The likelihood of targeting is higher if the person is famous, or has many social media followers, or an OG username, or holds a large amount of money or cryptocurrency.

Indicators of Takeover

Affected phones cannot make calls, have no reception, and potentially have no 911 access. Additionally, attackers take over online accounts belonging to the subscriber. Unexpected text messages or e-mails referring to password resets, account logins, or phone number changes may occur before a successful takeover.

Mitigations

The major challenge with mitigating against this attack vector is that the flaw resides on a website owner's authentication logic, over which the user has no control. Multifactor authentication involves something you know, something you have, and something you are. Traditional authentication only required something you know, such as a password or a PIN. Online 2FA typically requires a combination of the password and something you have, such as a physical token or other object that cannot be stolen by a remote attacker.

In the case of many online services, 2FA treats possession of a phone number as something you have, which SIM swap fraud exploits. For many websites, the phone number is also often a password recovery mechanism, effectively reducing the whole thing to one factor if the phone number can be easily taken over. In July 2016, the National Institute of Standards and Technology (NIST) stated SMS was to be deprecated for use in 2FA. NIST later issued revised guidance, stating, "the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device," citing "SIM change" as a risk factor. Though NIST published these recommendations, websites that use SMS-based 2FA cannot obtain the private information necessary to determine that, so they cannot mitigate those risk factors.

Additionally, phone numbers exist in limited quantities and dropped numbers are re-allocated to new customers. Since website owners typically cannot determine if a phone number has a new owner, over time, random people can gain control over accounts by receiving a recycled number.

As a result, any mitigations initiated by the end user are suboptimal, and can increase the risk from other types of account takeover vectors, or simple account loss from a forgotten password. The website owner is the only party that can fix these flaws, and it involves deprecating the use of phone number as a password recovery option and its use in 2FA.

The most effective fix is likely for the website owner to require hardware or software 2FA for online accounts. For websites that require the use of phone numbers, the end user could use Google Voice and other voice over internet protocol (VoIP) providers, that are likely less susceptible to SIM swap fraud. Some websites deliberately block the use of VoIP numbers and will only accept numbers from a traditional cellular carrier. In this case, if the account is worth the effort, the end user can set up a new mobile phone with a new, secret phone number that is only used for this purpose. After the phone number is added, the user can then port it over to Google Voice, where it is less susceptible to SIM swap fraud. However, for many end users, such measures may be considered too involved or impractical for securing all of their online accounts, particularly when taking into account the largely targeted nature of most SIM swap fraud operations. For individuals believed to have elevated risk of such targeting, measures such as these may be necessary.

On some websites that allow phone number-based password recovery, completely removing the phone number from the account can reduce the risk from SIM swap fraud. This can, however, increase the risk from other types of account takeover and loss.

Some information has been redacted from this report in order to protect sources.

Flashpoint Analyst Team

The Flashpoint analyst team is composed of subject-matter experts with tradecraft skills honed through years of operating in the most austere online environments, training in elite government and corporate environments, and building and leading intelligence programs across all sectors. Our team covers more than 20 languages including Arabic, Mandarin, Farsi, Turkish, Kazakh, Spanish, French, German, Russian, Ukrainian, Italian, and Portuguese.

MARKETS

Why crypto investors might want to think twice about giving out their phone numbers

PUBLISHED SAT, AUG 18 2018•11:21 AM EDT UPDATED SAT, AUG 18 2018•12:56 PM EDT

Kate Rooney
@KROONEY

SHARE

KEY POINTS

Hackers are using a method known as “SIM swapping” to steal phone numbers and in some cases, use them to take millions of dollars worth of cryptocurrency.

This week, a California man sued his wireless carrier AT&T for $224 million after criminals used the method to steal $24 million from an cryptocurrency exchange.

“Once hackers get access to your private keys, they own your money and you’re screwed,” says Kyle Samani, managing partner at Multicoin Capital.

Why crypto investors might want to think twice about giving out their phone numbers

It's a familiar scenario.

You forget a password to a website or log in from a new computer, and get locked out of your account. The website or your bank sends a text to confirm it's you. Most of the time it is.

But the person receiving that text could be a hacker. Criminals are using a method known as "SIM swapping" to take over phone number accounts by duping wireless carriers, and in some cases stealing millions of dollars worth of cryptocurrency.

"In online banking, if someone gets into your account there's ways to get the money back," said Kyle Samani, managing partner at crypto hedge fund Multicoin Capital. "In crypto, if hackers get access to your your private keys, they own your money and you're screwed."

This week, a California man sued AT&T for $224 million after hackers used his number to steal $24 million worth of cryptocurrency stored on an online exchange. The plaintiff Michael Terpin accused AT&T of negligence, and likened

it to "a hotel giving a thief with a fake ID a room key and a key to the room safe to steal jewelry in the safe from the rightful owner."

Terpin is hardly the only one to suffer a hack. The total in cryptocurrency lost by individuals hit $1.6 billion at the end of June, according to CoinDesk's 2018 State of Blockchain Report.

In order to stop the trend, cybersecurity and industry experts say investors should guard their cellphone numbers with the same paranoia with which they guard their social security numbers.

Swapping digits

Wireless store employees can assign your phone number to any device, with the right authorization. To confirm, they ask for pieces of private information like a birthday or a social security number. But those can be easily accessed for a price.

"Data is being bought, sold and traded on the dark web," said Aaron Higbee, chief technology officer and co-founder of anti-phishing company Cofense. "If your phone number is of a sufficient age, you're on a database somewhere."

While one piece of data like a birthday might not be valuable on its own, combined with your phone number or address it can be used to answer those security questions from a wireless store employee.

After a criminal hacks into the person's email or cryptocurrency account from their own devices, what's known as "two-factor identification" will send a text code to the phone number as a form of security, and to prevent any sort of unauthorized log in. But because the hacker now controls that phone number, there's no way of the rightful owner regaining control or stopping the hack.

This happened to a New York-based venture capitalist who invests in early stage tech companies. He asked not to be named for this story because he did not want to be targeted again, and feared he might egg on the hackers.

He was in his office on Monday when he was suddenly logged out of both his personal and business email accounts. When he turned on his AT&T phone, the device had no signal. Because of his experience in cryptocurrency and the tech world, he recognized it as a SIM swap attack. He immediately called his wireless carrier through Skype, and quickly went to the store to regain access to his cell phone but "not quickly enough."

"This was the perfect storm," he said. "If I was on vacation or didn't know what to do immediately, they would have taken everything in my bank account."

He was able to regain control of his email but not his Coinbase account. Hackers had already moved the cryptocurrency he held to another account, and had attempted to wire money from his CitiBank account, which was refunded by the bank, he said.

The total amount stolen was roughly $5,000 — which he says is no where near the total of his crypto holdings because the rest was stored offline.

Keeping funds offline

Savvy, and in some cases paranoid, crypto investors opt to keep their funds in what's known as "cold storage." The method allows you to store digital currency offline, away from any internet access and therefore makes it harder to hack.

Cryptocurrency exchange Abra does not store any of its customers funds online for this very reason, according to CEO Bill Barhydt. He called storing private keys online "the worst idea in the history of bad ideas." Those who want to keep money on an exchange might be trading it frequently, or could be first-time investors who bought in when bitcoin became a household-name in December. The cryptocurrency climbed to nearly $20,000, inviting a wave of first-time retail investors.

Private keys are the only way to access cryptocurrency wallets online. In many cases, people use their phone numbers as the only backup if they forget that code.

"Your phone number right now is a lot more important than your social security number," Barhydt said. "The average consumer doesn't pay attention to security until they've been hacked."

Wireless carriers

It's still unclear who is legally responsible when a phone number is used to hack into a cryptocurrency account. Exchanges say the customer, and angry customers have blamed exchanges or in the case of Michael Terpin, his wireless carrier.

"The question is, do people believe that telecos have responsibility for protecting your bank account? Maybe that's a little much to ask," said Stephen Palley, partner at Anderson Kill and co-chair of the firm's blockchain and virtual

currency group. “A telecommunication company doesn’t have control over what you use your phone for.”

Still, Terpin is seeking damages from AT&T, which told CNBC in an emailed statement, “We dispute these allegations and look forward to presenting our case in court.”

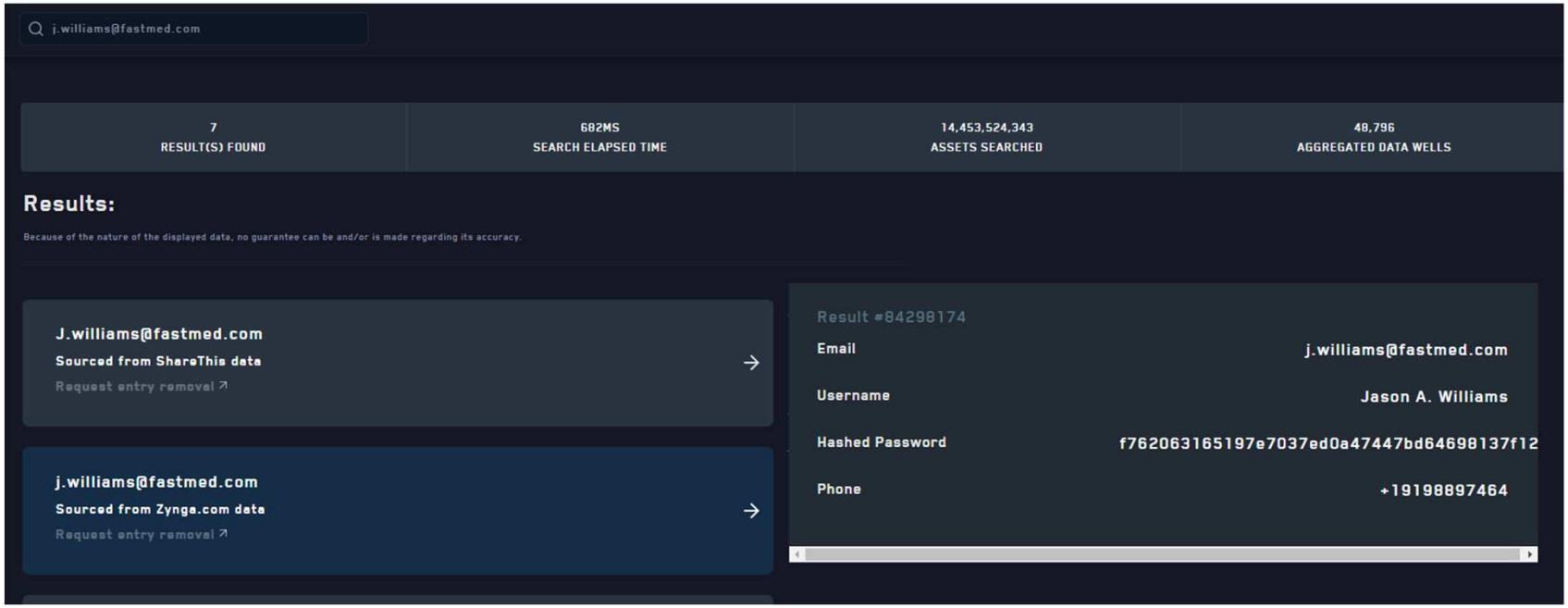
It’s not just cryptocurrency at risk. Palley said anything for which a cell phone is used as a second way to identify yourself could be at risk if a hacker takes over your phone number.

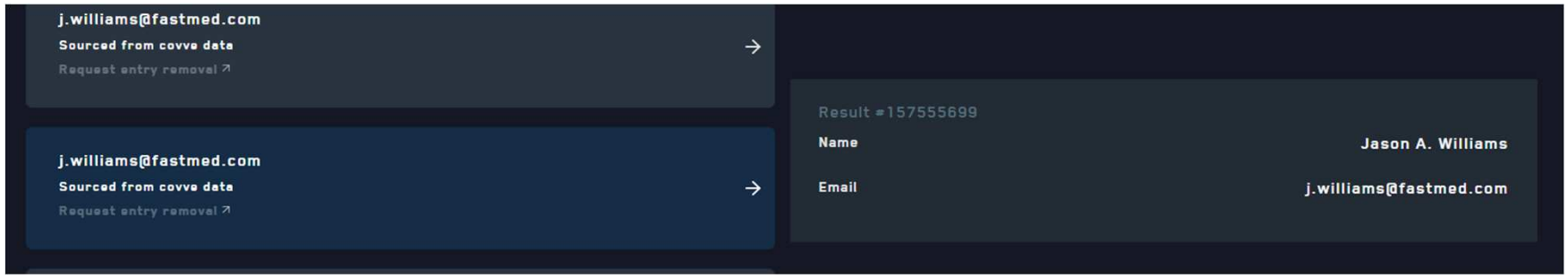
“People assume that your cell phone is a comfortable and secure way of protecting data,” he said. “It turns out that it’s not.”

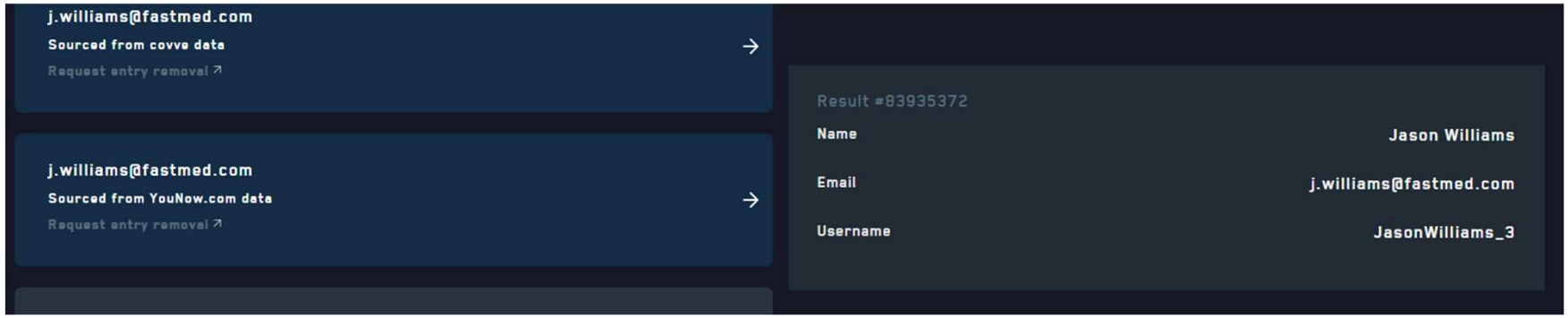
If you’re worried about a hack:

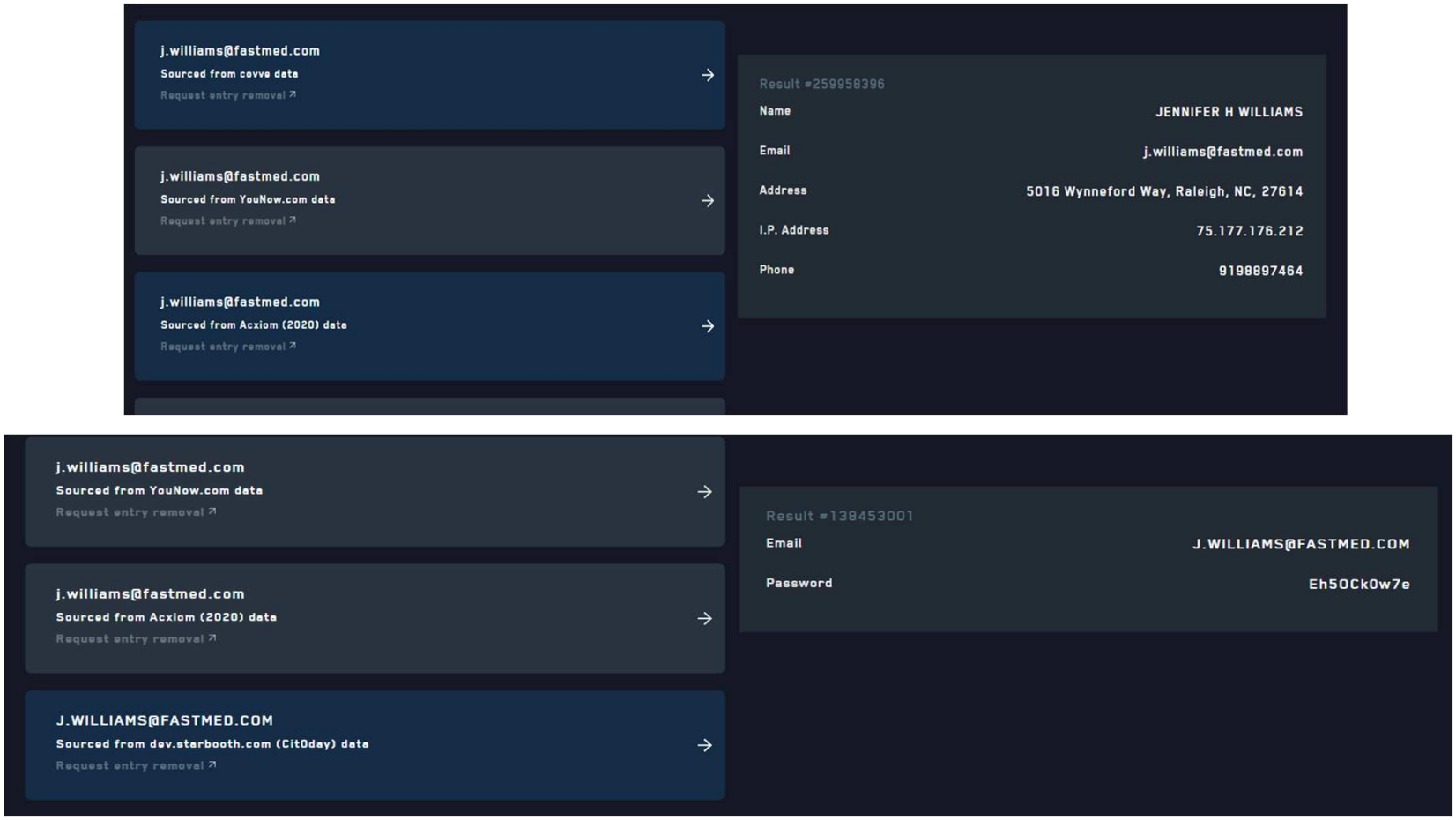
- Consider alternative authentication applications. Cofense’s Aaron Higbee recommended apps like Google Authenticator, Microsoft Authenticator, Authy, Duo, or Authenticator plus.
- Don’t store your cryptocurrency on an exchange for extended periods of time, according to Multicoin Capital’s Kyle Samani.
- Call your service provider and request additional protections on your account.
- Consider the risks: “I don’t think it’s appropriate to walk around with your life savings on a crypto wallet in your pocket,” Higbee says.
- Don’t go bragging about your crypto gains and Lamborghini, or #lambo, on Twitter. “What you’re doing is saying I have all of this money, so hack me personally,” says Higbee.
- Don’t post a screenshot that includes your wireless carrier (it will usually show up in the top left corner of your phone). Higbee says this applies more to celebrities, who might not want curious wireless employees snooping into their accounts.
- Don’t post your cellphone number online.

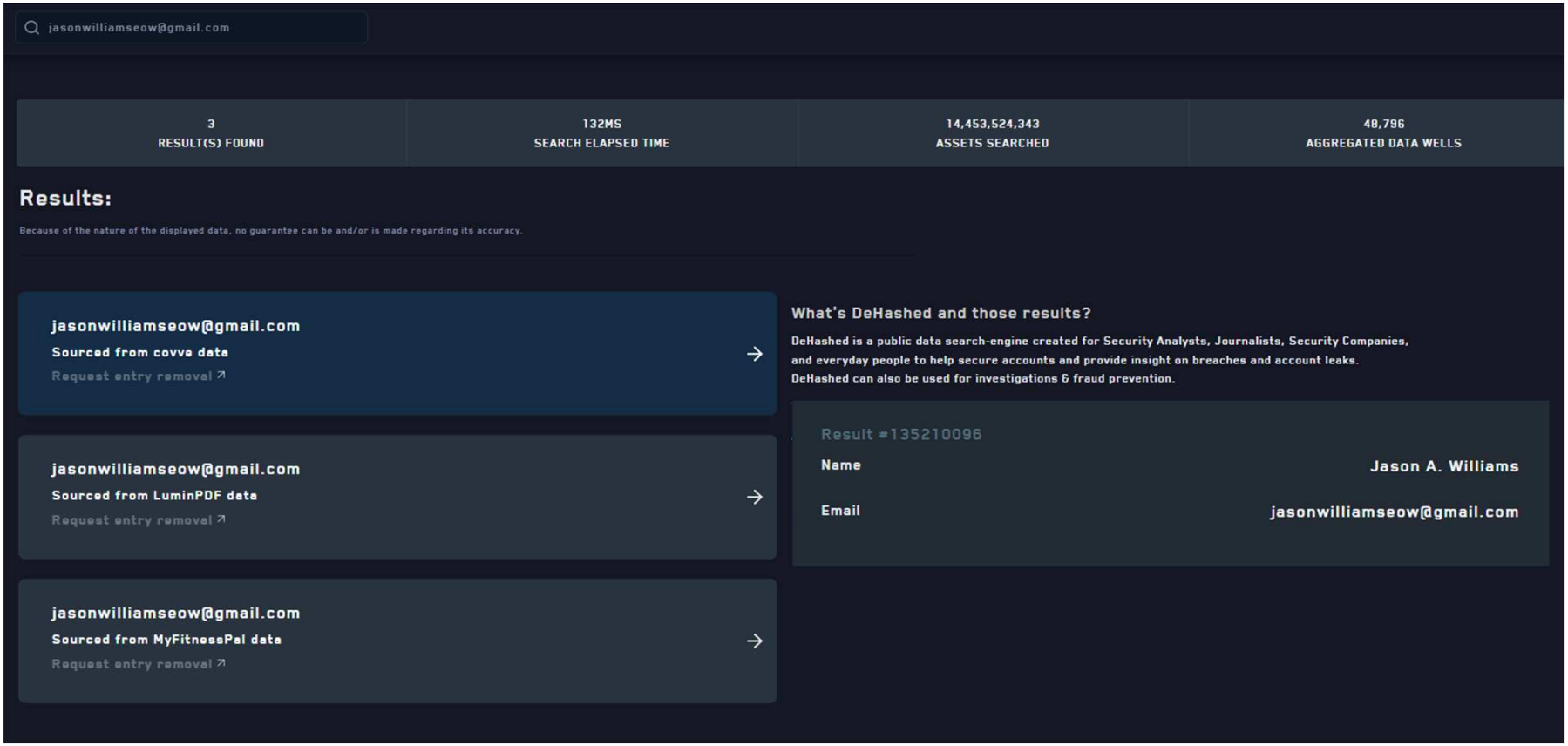
EXHIBIT D

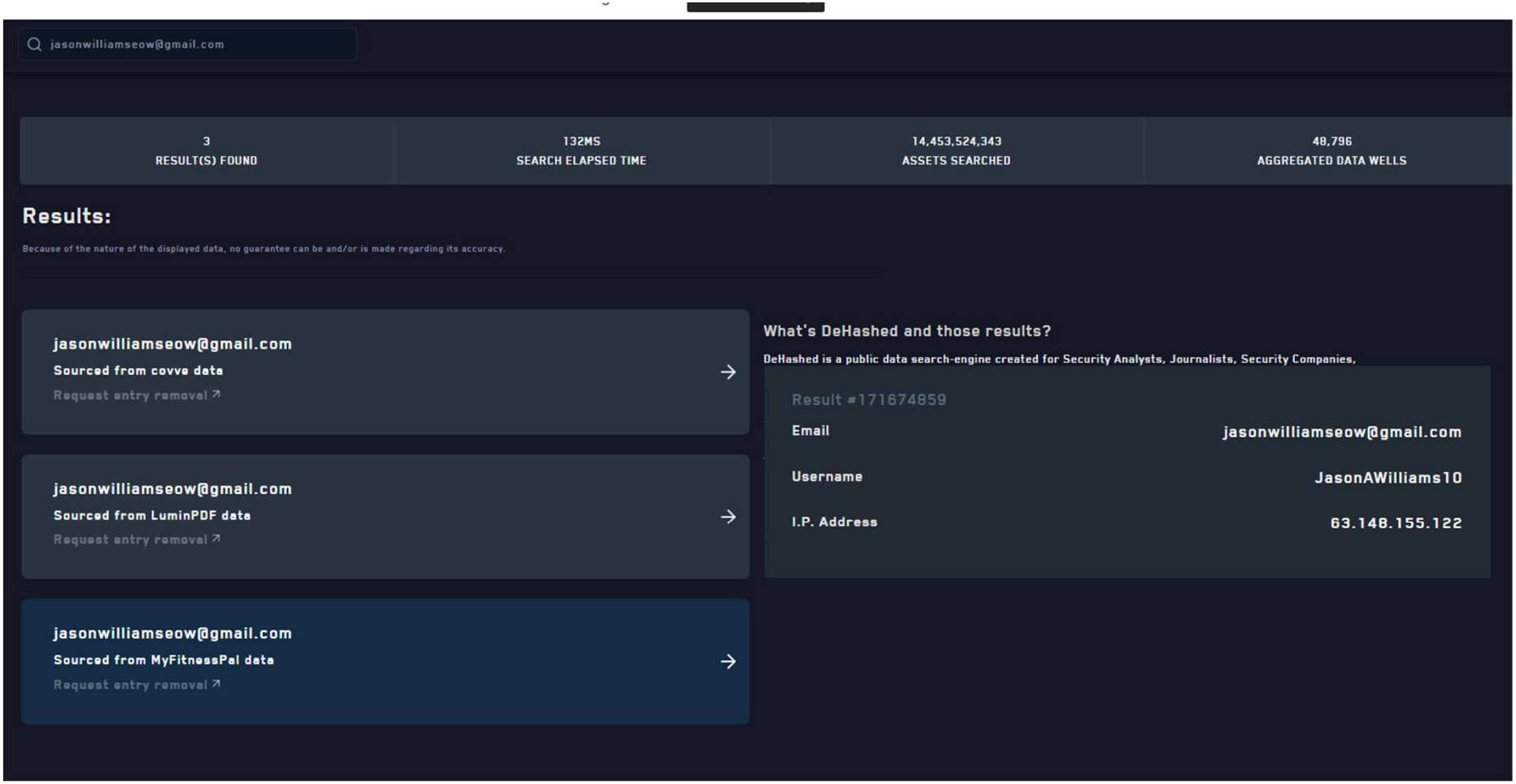

j.williams@fastmed.com
7
RESULT(S) FOUND
682MS
SEARCH ELAPSED TIME
14,453,524,343
ASSETS SEARCHED
48,796
AGGREGATED DATA WELLS
Results:
Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.
J.williams@fastmed.com
Sourced from ShareThis data
Request entry removal
j.williams@fastmed.com
Sourced from Zynga.com data
Request entry removal
Result #84298174
Email
j.williams@fastmed.com
Username
Jason A. Williams
Hashed Password
f762063165197e7037ed0a47447bd64698137f12
Phone
+19198897464

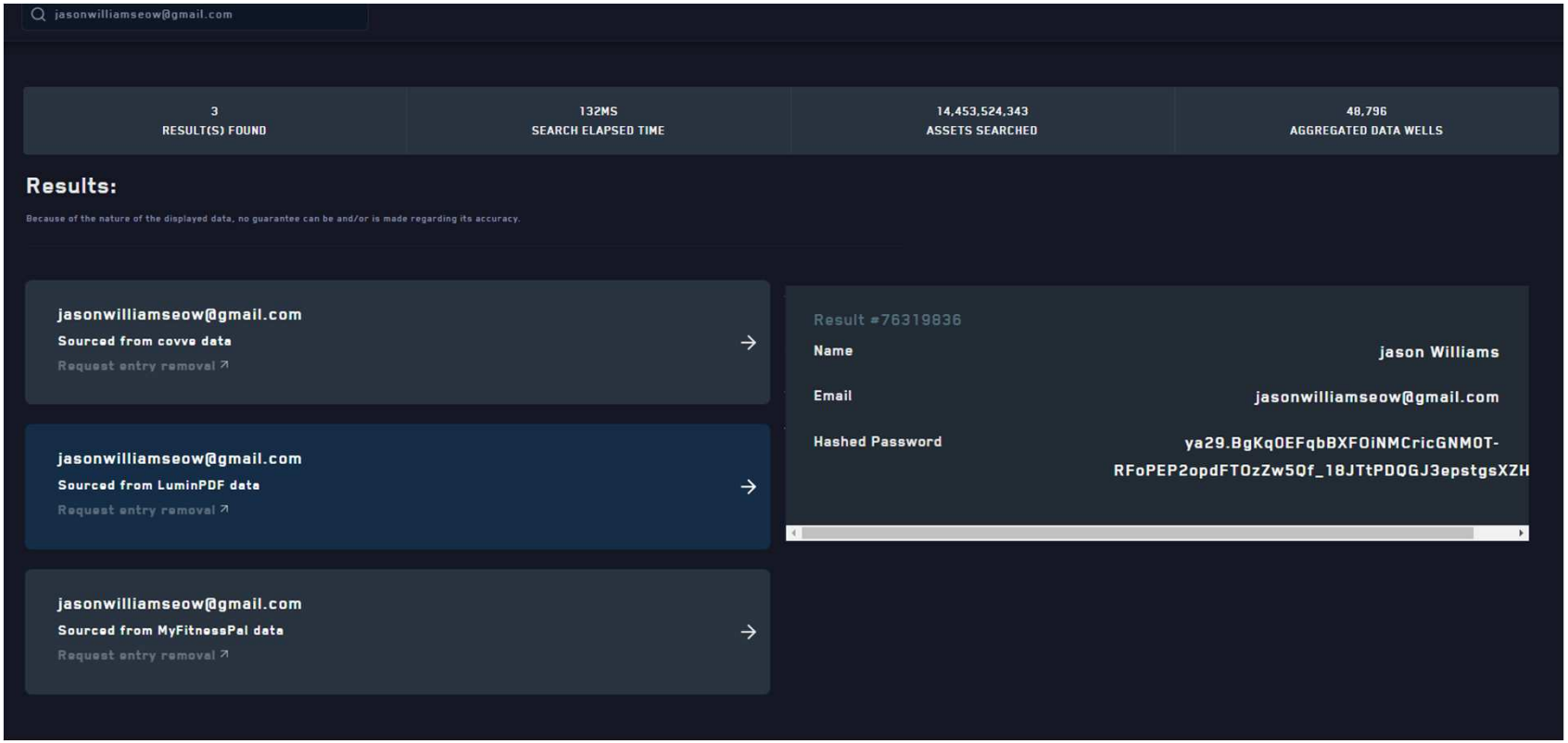

j.williams@fastmed.com
Sourced from covve data
Request entry removal
j.williams@fastmed.com
Sourced from covve data
Request entry removal
Result #157555699
Name
Jason A. Williams
Email
j.williams@fastmed.com


j.williams@fastmed.com
Sourced from covve data
Request entry removal
j.williams@fastmed.com
Sourced from YouNow.com data
Request entry removal
Result #83935372
Name
Jason Williams
Email
j.williams@fastmed.com
Username
JasonWilliams_3


j.williams@fastmed.com
Sourced from covve data
Request entry removal
j.williams@fastmed.com
Sourced from YouNow.com data
Request entry removal
j.williams@fastmed.com
Sourced from Acxiom (2020) data
Request entry removal
Result #259958396
Name
JENNIFER H WILLIAMS
Email
j.williams@fastmed.com
Address
5016 Wynneford Way, Raleigh, NC, 27614
I.P. Address
75.177.176.212
Phone
9198897464
j.williams@fastmed.com
Sourced from YouNow.com data
Request entry removal
j.williams@fastmed.com
Sourced from Acxiom (2020) data
Request entry removal
J.WILLIAMS@FASTMED.COM
Sourced from dev.starbooth.com (CitOday) data
Request entry removal
Result #138453001
Email
J.WILLIAMS@FASTMED.COM
Password
Eh5OCkOw7e


jasonwilliamseow@gmail.com
3
RESULT(S) FOUND
132MS
SEARCH ELAPSED TIME
14,453,524,343
ASSETS SEARCHED
48,796
AGGREGATED DATA WELLS
Results:
Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.
jasonwilliamseow@gmail.com
Sourced from covve data
Request entry removal
jasonwilliamseow@gmail.com
Sourced from LuminPDF data
Request entry removal
jasonwilliamseow@gmail.com
Sourced from MyFitnessPal data
Request entry removal
What's DeHashed and those results?
DeHashed is a public data search-engine created for Security Analysts, Journalists, Security Companies, and everyday people to help secure accounts and provide insight on breaches and account leaks.
DeHashed can also be used for investigations & fraud prevention.
Result #135210096
Name
Jason A. Williams
Email
jasonwilliamseow@gmail.com


jasonwilliamseow@gmail.com
3
RESULT(S) FOUND
132MS
SEARCH ELAPSED TIME
14,453,524,343
ASSETS SEARCHED
48,796
AGGREGATED DATA WELLS
Results:
Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.
jasonwilliamseow@gmail.com
Sourced from covve data
Request entry removal
jasonwilliamseow@gmail.com
Sourced from LuminPDF data
Request entry removal
jasonwilliamseow@gmail.com
Sourced from MyFitnessPal data
Request entry removal
What's DeHashed and those results?
DeHashed is a public data search-engine created for Security Analysts, Journalists, Security Companies,
Result #171674859
Email
jasonwilliamseow@gmail.com
Username
JasonAWilliams10
I.P. Address
63.148.155.122


jasonwilliamseow@gmail.com
3
RESULT(S) FOUND
132MS
SEARCH ELAPSED TIME
14,453,524,343
ASSETS SEARCHED
48,796
AGGREGATED DATA WELLS
Results:
Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.
jasonwilliamseow@gmail.com
Sourced from covve data
Request entry removal
jasonwilliamseow@gmail.com
Sourced from LuminPDF data
Request entry removal
jasonwilliamseow@gmail.com
Sourced from MyFitnessPal data
Request entry removal
Result #76319836
Name
jason Williams
Email
jasonwilliamseow@gmail.com
Hashed Password
ya29.BgKqOEFqbBXFOiNMCricGNMOT-RFoPEP2opdFTOzZw5Qf_18JTtPDQGJ3epstgsXZH

truthfinder

Background Report

Jason Anthony Williams

Link to Report

Report Created

Jan 23, 2021

truthfinder.com/dashboard

Disclaimer

TruthFinder IS NOT A CREDIT REPORTING AGENCY ("CRA") FOR PURPOSES OF THE FAIR CREDIT REPORTING ACT ("FCRA"), 15 USC §§ 1681 et seq. AS SUCH, THE ADDITIONAL PROTECTIONS AFFORDED TO CONSUMERS, AND OBLIGATIONS PLACED UPON CREDIT REPORTING AGENCIES, ARE NOT CONTEMPLATED BY, NOR CONTAINED WITHIN, THESE TERMS.

You may not use any information obtained from this report in connection with determining a prospective candidate's suitability for:

- Health insurance or any other insurance
- Credit and/or loans
- Employment
- Education, scholarships or fellowships
- Housing or other accommodations
- Benefits, privileges or services provided by any business establishment.

The information provided by this report has not been collected in whole or in part for the purpose of furnishing consumer reports, as defined in the FCRA. Accordingly, you understand and agree that you will not use any of the information you obtain from this report as a factor in: (a) establishing an individual's eligibility for personal credit, loans, insurance or assessing risks associated with existing consumer credit obligations; (b) evaluating an individual for employment, promotion, reassignment or retention (including employment of household workers such as babysitters, cleaning personnel, nannies, contractors, and other individuals); (c) evaluating an individual for educational opportunities, scholarships or fellowships; (d) evaluating an individual's eligibility for a license or other benefit granted by a government agency or (e) any other product, service or transaction in connection with which a consumer report may be used under the FCRA or any similar state statute, including, without limitation, apartment rental, check-cashing, or the opening of a deposit or transaction account. You also agree that you shall not use any of the information you receive through this report to take any "adverse action," as that term is defined in the FCRA; you have appropriate knowledge of the FCRA; and, if necessary, you will consult with an attorney to ensure compliance with these Terms.

Personal Information

This section contains known aliases, birth information, and potential imposters gleaned from public records.

First Name	Middle Name	Last Name
Jason	Anthony	Williams

Birth Information

Age	Birth Date
46	Mar 11, 1974

Known Aliases

Jason Anthon Williams

Jobs

Company (Industry)	Job Title	Dates
Morgan Creek Digital Assets	Co Founder and General Partner	Apr 10, 2020 - May 26, 2020
Morgan Creek Digital Assets (Venture Capital & Private Equity)	Partner	Nov 3, 2018 - Dec 26, 2019
Morgan Creek Blockchain Capital	Partner	Nov 3, 2018 - Nov 3, 2018
RTP Capital Associates, Inc.	Angel Investor	Oct 1, 2016 - May 26, 2020
Duke Angel Network	Angel Investor	Oct 1, 2016 - May 26, 2020
Full Tilt Capital	Managing Partner	Aug 17, 2017 - May 26, 2020
Louisburg College	Member Board of Trustess	Jul 13, 2016 - May 26, 2020
Undercover Colors	Angel Investor	Jul 13, 2016 - May 26, 2020
Duke University School of Medicine	Advisor to Innovations in Healthcare	Jul 13, 2016 - May 26, 2020
Fortnight Brewing	Angel Investor	Jul 13, 2016 - May 26, 2020
FishBetter	Angel Investor	Jan 22, 2016 - May 26, 2020
Angel investor - Social Entrepreneur	Healthcare Catalyst and Team Builder	Oct 2, 2015
PRTI Inc	Member of the Board of Directors	Jul 13, 2016 - May 26, 2020
PRTI Inc	Angel Investor / President / Board Member	Oct 2, 2015
Penda Health	Angel Investor	Oct 2, 2015 - May 26, 2020
Duke University	Innovations in Healthcare	May 26, 2020 - May 26, 2020
PRTI	President and CEO	Jan 22, 2016 - May 26, 2020
Dermasensa Laboratories	Angel Investor	Oct 2, 2015 - May 26, 2020
JuiceVibes	Angel Investor	Oct 2, 2015 - May 26, 2020
13C Molecular	Angel Investor	Oct 2, 2015 - May 26, 2020
Methodist University	Member Board of Trustees	Jul 13, 2016 - May 26, 2020
Pierros Italian Bistro	Angel Investor	Oct 2, 2015 - May 26, 2020

FastMed	Founder and Former President and CEO, President and CEO of the Eastern Region	Oct 2, 2015 - May 26, 2020
PhyAmerica	Emergency Physician Assistant	Oct 2, 2015
Cape Fear Orthopedics	Orthopedic Surgical Physician Assistant	Oct 2, 2015
N/A (Offices Of Health Practitioner)	Physician Assistant	Jan 1, 2008
BOONE UC INC	OWNER	Sep 16, 2020 - Sep 16, 2020

Education

Attendance Dates	Qualification Type	University
Jan 1, 2010 - Dec 31, 2010	Doctor of Humanities, honoris causa	Methodist University
Jan 1, 2002 - Dec 31, 2004	Master's Degree, Master of Physician Assistant Studies	University Of Nebraska-lincoln
Jan 1, 1998 - Dec 31, 1999	Surgical training, Advanced Training in General Surgery	Yale University School Of Medicine
Jan 1, 1996 - Dec 31, 1998	Bachelor of Health Science (BHS), Physician Assistant	Methodist University
Jan 1, 1992 - Dec 31, 1998	Bachelor of Science (B.S.), Human Biology	Methodist University

Possible Relatives

Name	Age	Date of Birth
Veronica Bertha Williams	71 (approx)	Jan 1, 1950 - Dec 31, 1950
Jennifer Hutson Williams	48 (approx)	Jan 1, 1973 - Dec 31, 1973
Arris Tayron Williams	41 (approx)	Jan 1, 1980 - Dec 31, 1980
Joseph T Lorenzo	66 (approx)	Jan 1, 1955 - Dec 31, 1955
Jason Williams	N/A	N/A

Possible Associates

Jacqueline Susanne Lorenzo, 67 years old (approximate)

Shared Locations

Phone Numbers (772) 215-1444
(772) 286-8832
(772) 545-1964

1902 Se Erwin Rd

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Oct 01, 1997 to Jan 23, 2003 for 5 years 3 months 25 days

3212 Se Aster Ln Apt Q210

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Feb 01, 2000 to Dec 13, 2009 for 9 years 10 months 18 days

1014 Clarendon St

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Dec 01, 2007 to Jan 14, 2008 for 1 months 14 days

6051 Se Riverboat Dr

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Jul 01, 1994 to Jan 23, 2003 for 8 years 6 months 28 days

180 Se Placita Ct

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Nov 22, 1998 to Jan 23, 2003 for 4 years 2 months 3 days

6061 Se Riverboat Dr

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Sep 01, 1997 to Jan 23, 2003 for 5 years 4 months 25 days

2713 Preston Woods Ln Apt 7

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Sep 22, 2000 to Dec 01, 2001 for 1 years 2 months 10 days

901 Tallstone Dr

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Jul 01, 1999 to Jul 07, 1999 for 6 days

6055 Se Riverboat Dr

Jacqueline Susanne Lorenzo and Jason Anthony Williams may have shared this address from Jul 01, 1994 to Sep 15, 1997 for 3 years 2 months 17 days

Paul D Fisher, 75 years old (approximate)

Shared Locations

Phone Numbers

(772) 220-0394

(561) 219-3742

(561) 219-3743

PO Box 2702

Paul D Fisher and Jason Anthony Williams may have shared this address from Jun 25, 1994 to Jan 23, 2003 for 8 years 7 months 4 days

1902 Se Erwin Rd

Paul D Fisher and Jason Anthony Williams may have shared this address from Oct 01, 1997 to Jan 23, 2003 for 5 years 3 months 25 days

6051 Se Riverboat Dr

Paul D Fisher and Jason Anthony Williams may have shared this address from Dec 17, 1994 to Jan 23, 2003 for 8 years 1 months 9 days

6055 Se Riverboat Dr

Paul D Fisher and Jason Anthony Williams may have shared this address from Jul 01, 1994 to Apr 04, 1997 for 2 years 9 months 8 days

Mary Anna Montore, 92 years old (approximate)

Shared Locations

6061 Se Riverboat Dr

Mary Anna Montore and Jason Anthony Williams may have shared this address from Jul 01, 1994 to Jan 23, 2003 for 8 years 6 months 28 days

1014 Clarendon St

Mary Anna Montore and Jason Anthony Williams may have shared this address from Sep 01, 2007 to Mar 01, 2012 for 4 years 6 months 3 days

6011 Se Riverboat Dr

Mary Anna Montore and Jason Anthony Williams may have shared this address from Jul 01, 1994 to Jan 23, 2003 for 8 years 6 months 28 days

Phone Numbers

(772) 692-2467
(407) 283-9424
(516) 872-2990
(561) 283-9424
(561) 335-4790
(561) 692-2042
(561) 692-4765
(772) 692-2288
(772) 905-8530
(772) 971-2016
(910) 484-9405

Louis Montore, 93 years old (approximate)

Shared Locations

6061 Se Riverboat Dr

Louis Montore and Jason Anthony Williams may have shared this address from Jul 01, 1994 to Jan 23, 2003 for 8 years 6 months 28 days

Phone Numbers

(561) 283-9424
(772) 283-9424
(954) 975-2575

Bruce Allan Sloan, 63 years old (approximate)

Shared Locations

Phone Numbers

180 Se Placita Ct

Bruce Allan Sloan and Jason Anthony Williams may have shared this address from Nov 22, 1998 to Jan 23, 2003 for 4 years 2 months 3 days

(386) 864-1220
(561) 232-1212
(561) 232-1611
(561) 337-3740
(561) 343-0326
(772) 232-1212
(772) 781-8729
(904) 343-0326

Denise McGuire, 62 years old (approximate)

Shared Locations

180 Se Placita Ct

Denise McGuire and Jason Anthony Williams may have shared this address from Nov 22, 1998 to Jan 23, 2003 for 4 years 2 months 3 days

Phone Numbers

(772) 873-2269
(772) 260-0954
(267) 222-8755
(561) 343-0326
(561) 781-8729
(772) 781-8729
(772) 812-0249
(772) 877-8444
(904) 343-0326
(954) 873-6237
(724) 567-7501

Donna Marie Walker, 51 years old (approximate)

Shared Locations

PO Box 2702

Donna Marie Walker and Jason Anthony Williams may have shared this address from Apr 01, 1995 to Jan 23, 2003 for 7 years 9 months 29 days

Phone Numbers

(772) 985-6901
(561) 219-9568
(561) 253-2733
(772) 219-9568
(772) 220-0394
(772) 241-3078
(772) 419-3078
(772) 626-2036
(772) 626-2039
(772) 626-2741
(772) 807-5799
(772) 919-5954
(772) 253-2733

Kathleen M Fisher, 64 years old (approximate)

Shared Locations

PO Box 2702

Kathleen M Fisher and Jason Anthony Williams may have shared this address from Dec 03, 1995 to Jan 23, 2003 for 7 years 1 months 23 days

PO Box 2703

Phone Numbers

(772) 220-0394

Terese Mary Lorenzo, 46 years old (approximate)

Phone Numbers
(252) 996-0190

Myrtle Wilson Vann, 101 years old (approximate)

Shared Locations
1014 Clarendon St
Myrtle Wilson Vann and Jason Anthony Williams may have shared this address from Mar 01, 2003 to Jun 05, 2018 for 15 years 3 months 9 days
1010 Clarendon St

Phone Numbers
(910) 485-1734
(910) 321-0066
(919) 803-8105

Matthew Glenn Hudson, 33 years old (approximate)

Shared Locations
1010 Clarendon St

Phone Numbers
(910) 309-6452
(336) 213-5132
(336) 971-8958
(910) 486-0730
(843) 234-1721

Manuel J Varela, 54 years old (approximate)

Phone Numbers
(561) 223-0916
(561) 287-4586

Jennifer Sparling McDonald, 48 years old (approximate)

Shared Locations
2713 Preston Woods Ln Apt 7
Jennifer Sparling McDonald and Jason Anthony Williams may have shared this address from Jun 01, 2000 to Dec 01, 2004 for 4 years 6 months 4 days

Phone Numbers
(910) 323-0054
(910) 484-7174
(312) 399-1649

Shannon Michael McDonald, 47 years old (approximate)

Shared Locations
2713 Preston Woods Ln Apt 7
Shannon Michael McDonald and Jason Anthony Williams may have shared this address from Feb 01, 2004 to Dec 01, 2004 for 10 months 4 days

Phone Numbers
(919) 219-0228
(910) 484-7174
(919) 777-0693
(919) 349-3956

Yeny Garay, 39 years old (approximate)

Shared Locations
180 Se Placita Ct

Phone Numbers
(561) 463-7580

(561) 781-2214
(772) 463-7580

Gregory Louis Doyle, 69 years old (approximate)

Shared Locations

PO Box 2703

Gregory Louis Doyle and Jason Anthony Williams may have shared this address from Jan 13, 1996 to Jan 23, 2003 for 7 years 12 days

PO Box 2702

Gregory Louis Doyle and Jason Anthony Williams may have shared this address from Jan 01, 1996 to Jan 23, 2003 for 7 years 24 days

Phone Numbers

(772) 286-6987
(954) 937-9322
(407) 286-6987
(419) 747-1607
(561) 286-6987

Eva Thieme Hudson, 61 years old (approximate)

Shared Locations

1010 Clarendon St

Eva Thieme Hudson and Jason Anthony Williams may have shared this address from Mar 01, 2003 to Jun 05, 2018 for 15 years 3 months 9 days

Phone Numbers

(910) 308-7778
(910) 779-1164
(910) 379-9643
(910) 309-0188
(910) 486-0730
(919) 779-1164

Mickey Glenn Hudson, 58 years old (approximate)

Shared Locations

1010 Clarendon St

Mickey Glenn Hudson and Jason Anthony Williams may have shared this address from Mar 01, 2003 to Jun 05, 2018 for 15 years 3 months 9 days

Phone Numbers

(910) 486-0730
(910) 308-7778
(910) 309-0188
(404) 343-3503
(404) 695-0394
(678) 422-5569
(910) 379-9643
(910) 779-1164
(919) 779-1164

Maria Anna Lorenzo, 65 years old (approximate)

(772) 971-2016

Helen Mae Cooke, 96 years old (approximate)

Shared Locations

1902 Se Erwin Rd

Helen Mae Cooke and Jason Anthony Williams may have shared this address from Oct 01, 1997 to Jan 23, 2003 for 5 years 3 months 25 days

Phone Numbers

(803) 775-1446
(304) 775-1446
(304) 778-6895
(304) 846-2915
(561) 220-9229
(772) 220-9229
(803) 778-6895
(803) 934-0178

Wayne Douglas Cook, 78 years old (approximate)

Shared Locations

1902 Se Erwin Rd

Wayne Douglas Cook and Jason Anthony Williams may have shared this address from Oct 01, 1997 to Jan 23, 2003 for 5 years 3 months 25 days

Phone Numbers

(772) 220-9229
(407) 220-3777
(561) 335-7255
(772) 220-3777
(772) 220-6663
(772) 220-7599
(772) 398-4767

Phillip G Cooke, 101 years old (approximate)

Shared Locations

1902 Se Erwin Rd

Phillip G Cooke and Jason Anthony Williams may have shared this address from Oct 01, 1997 to Jan 23, 2003 for 5 years 3 months 25 days

Phone Numbers

(772) 220-9229
(772) 626-6338

Dana Michelle Craft, 43 years old (approximate)

Shared Locations

180 Se Placita Ct

Dana Michelle Craft and Jason Anthony Williams may have shared this address from Nov 22, 1998 to Jan 23, 2003 for 4 years 2 months 3 days

Phone Numbers

(984) 225-2100
(386) 423-3229
(407) 207-0780
(407) 281-6872
(407) 343-0326
(407) 563-2411
(407) 879-6099
(772) 879-6099
(904) 207-0780
(904) 423-3229
(772) 971-6641

Alba Varela Heysquierdo, 59 years old (approximate)

Shared Locations	180 Se Placita Ct Alba Varela Heysquierdo and Jason Anthony Williams may have shared this address from Jan 01, 2001 to Jan 23, 2003 for 2 years 22 days	Phone Numbers	(772) 781-8462 (407) 221-9524 (772) 283-6918

Maria Christina Gryner, 53 years old (approximate)

Shared Locations	180 Se Placita Ct Maria Christina Gryner and Jason Anthony Williams may have shared this address from Mar 01, 2002 to Jan 23, 2003 for 10 months 28 days	Phone Numbers	(561) 221-9865 (772) 220-2083 (772) 283-6918 (772) 336-1013 (772) 463-7318 (772) 781-2214 (772) 785-9335 (772) 807-7684

James Shields Harper, 97 years old (approximate)

Shared Locations	1010 Clarendon St James Shields Harper and Jason Anthony Williams may have shared this address from Mar 01, 2003 to Jun 01, 2008 for 5 years 3 months 3 days	Phone Numbers	(910) 297-4913 (910) 485-5736

Edna Wilson Harper, 96 years old (approximate)

Shared Locations	1010 Clarendon St Edna Wilson Harper and Jason Anthony Williams may have shared this address from Mar 01, 2003 to Sep 01, 2012 for 9 years 6 months 6 days		

Lynette Sue Anderson, 59 years old (approximate)

		Phone Numbers	(561) 781-7867 (954) 566-4647 (954) 907-9037

Doris Maricela Lopez Varela, 59 years old (approximate)

Shared Locations	180 Se Placita Ct Doris Maricela Lopez Varela and Jason Anthony Williams may have shared this address from Oct 19, 2001 to Jan 23, 2003 for 1 years 3 months 6 days		

(830) 876-2480
(561) 785-9335

Possible Relationships

Jasyn Rymer

Contact Information

This section contains phone numbers, previous phone number and email addresses associated with Jason Anthony Williams.

Possible Phone Numbers

(919) 615-2132

Phone Carrier	Line Type	Carrier Location	Prepaid	Connected
Time Warner Cable Information Services (north Carolina) Llc Dba Time Warner Cable - Nc (tw Telecom)	Landline	Raleigh-Morgan St, NC 27529	No	No

(910) 480-0769

Phone Carrier	Line Type	Carrier Location	Prepaid	Connected
Carolina Telephone And Telegraph Company Llc Dba Centurylink (centurylink)	Landline	Fayetteville-Raleigh Rd-, NC 28301	No	No

(910) 223-1082

Phone Carrier	Line Type	Carrier Location	Prepaid	Connected
Carolina Telephone And Telegraph Company Llc Dba Centurylink (centurylink)	Landline	Fayetteville-Mcgilvary St-, NC 28301	No	No

Possible Emails

jasonwilliamseow@gmail.com jwilliams@louisburg.edu j.williams@fastmed.com

Location Information

This section includes all of the locations related to this person. Locations listed may include current residence, past residences, and places of work.

5016 Wynneford Way, Raleigh, NC 27614-9810

Dates Seen At Address
Apr 1, 2012 - Jan 22, 2021

Classification
Residential

Address Type
Street
Address Contains a Valid Primary Number Range

Is Deliverable
Yes

Is Receiving Mail
Yes

Phone Numbers
(919) 896-8094

1010 Clarendon St, Fayetteville, NC 28305-4847

Dates Seen At Address
Mar 1, 2003 - Jun 5, 2018

Subdivision
Highland Heights

Classification
Residential

Address Type
Street
Address Contains a Valid Primary Number Range

Is Deliverable
Yes

Is Receiving Mail
Yes

Phone Numbers
(910) 223-1082

5311 Tannat Ct Apt 401, Raleigh, NC 27612-4690

Dates Seen At Address
Mar 1, 2015 - May 31, 2018

Classification
Residential

Address Type
High-Rise
Address Contains Apartment or Building Sub-Units

Building
32 Apartments

Is Deliverable
Yes

Is Receiving Mail
Yes

2105 Us 1 Hwy, Franklinton, NC 27525-8710

Dates Seen At Address
Aug 1, 2017 - Jan 4, 2018

Classification
Residential

Address Type
Street
Address Contains a Valid Primary Number Range

Is Deliverable
Yes

Is Receiving Mail
Yes

3212 Se Aster Ln Apt Q210, Stuart, FL 34994-5553

Dates Seen At Address
Jun 1, 1993 - Sep 10, 2011

Subdivision
Village Stuart Condo

Classification
Residential

Address Type
High-Rise
Address Contains Apartment or Building Sub-Units

Building
8 Apartments

Is Deliverable
Yes

Is Receiving Mail
Yes

11373 Us Highway 70 W, Clayton, NC 27520

Dates Seen At Address
May 31, 2008 - Jun 30, 2008

Address Type

No Record Type Because
Address Did Not Make a
Valid Dpv Match

2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304-3660

Dates Seen At Address
Jun 1, 2000 - Dec 1, 2004

Subdivision
Preston Woods Condo

Classification
Residential

Address Type
High-Rise
Address Contains Apart-
ment or Building Sub-Units

Building
12 Apartments

Is Deliverable
Yes

Is Receiving Mail
Yes

901 Tallstone Dr, Fayetteville, NC 28311-1469

Dates Seen At Address
Jun 1, 1998 - Dec 31, 2003

Classification
Residential

Address Type
Street
Address Contains a Valid
Primary Number Range

Is Deliverable
Yes

Is Receiving Mail
Yes

180 Se Placita Ct, Port Saint Lucie, FL 34983-2028

Dates Seen At Address
Nov 22, 1998 - Jan 23, 2003

Subdivision
River Park Un

Classification
Residential

Address Type
Street
Address Contains a Valid
Primary Number Range

Is Deliverable
Yes

Is Receiving Mail
Yes

1902 Se Erwin Rd, Port Saint Lucie, FL 34952-5520

Dates Seen At Address
Oct 1, 1997 - Jan 23, 2003

Subdivision
South Port St Lucie

Classification
Residential

Address Type
Street
Address Contains a Valid
Primary Number Range

Is Deliverable
Yes

Is Receiving Mail
Yes

6051 Se Riverboat Dr, Stuart, FL 34997-1521

Dates Seen At Address
Jul 1, 1994 - Jan 23, 2003

Subdivision
River Pines Miles Grant

Classification
Residential

Address Type
Street
Address Contains a Valid
Primary Number Range

Is Deliverable
Yes

Is Receiving Mail
Yes

2702, PO Box, Stuart, FL 34995-2702

Dates Seen At Address
Jun 1, 1994 - Jan 23, 2003

Classification
Residential

Address Type
Post Office Box
Address is a PO Box
Record Type

Is Deliverable
Yes

Criminal Records

DISCLAIMER: The criminal record information contained in our reports may not be 100% accurate or complete. This is because the information is pulled from records maintained by government agencies and the information contained in those records may not be 100% accurate or complete. Please use this information as a starting point for your own due diligence and investigation.

Likely Criminal Records

Jason Anthony Williams

Match Rating Based On:

First Name, Middle Name, Last Name, Date Of Birth, Address, Age

Charges Filed Date	Source
Apr 17, 2013	ADMINISTRATIVE OFFICE OF COURTS (North Carolina)

Personal Details

First Name	Middle Name	Last Name	Age	Date of Birth
Jason	Anthony	Williams	46	Mar 11, 1974

Address	Drivers License State
1010 Clarendon St, Fayetteville, Cumberland	Nc

Physical Appearance

Complexion	Ethnicity
White	White

Apr 17, 2013 - Charges Filed - Not Specified

Charges Filed Date	Crime Classification	Offense Code	Offense Description	Case Type
Apr 17, 2013	I	NOT SPECIFIED	Not Specified	Infraction

Case Number
9102013IF000579

Oct 26, 2006 - Charges Filed - Not Specified

Charges Filed Date	Crime Classification	Offense Description	Case Type	Case Number
Oct 26, 2006	Nos	Not Specified	Criminal	2502006CR707074

Jason Anthony Williams

Match Rating Based On:

First Name, Middle Name, Last Name, Date Of Birth, Address, Age

Offense Date	Source
Oct 26, 2006	ADMINISTRATIVE OFFICE OF COURTS (North Carolina)

Personal Details

First Name	Middle Name	Last Name	Age	Date of Birth
Jason	Anthony	Williams	46	Mar 11, 1974

Address

1010 Clarendon St,
Fayetteville, Cumberland

Physical Appearance

Ethnicity

White

Oct 26, 2006 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Offense Code
Oct 26, 2006	Oct 26, 2006	Cumberland, NC	Misdemeanor	20-141(J1)
Offense Description	**Case Type**	**Case Number**	**Court Name**	**Disposition**
Arraigned:speeding-067/45	Traffic Misdemeanor	01250CUMBERLAND-2006CR707074	Cumberland	Dismissal Without Leave By Da

Disposition Date

Dec 5, 2006

Jason Anthony Williams

Match Rating Based On:

First Name, Middle Name, Last Name, Date Of Birth, Address, Age

Charges Filed Date	Source
Aug 22, 2009	ADMINISTRATIVE OFFICE OF COURTS DEMOGRAPHIC IN-FRACTIONS (North Carolina)

Personal Details

First Name	Middle Name	Last Name	Age	Date of Birth
Jason	Anthony	Williams	46	Mar 11, 1974

Address

1010 Clarendon St,
Fayetteville, Cumberland

Physical Appearance

Ethnicity

White

Aug 22, 2009 - Charges Filed -

Charges Filed Date	Crime Location	Case Number	Court Name
Aug 22, 2009	Iredell, NC	4802009708344IF	Iredell

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Offense Date	Source
Apr 10, 2004	SARASOTA COUNTY CIRCUIT COURT (Florida)

Personal Details

First Name	Last Name	Age	Date of Birth	Address
Jason	Williams	46	Mar 11, 1974	6023 26th St W # 114, Bradenton, Manatee

Apr 10, 2004 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Crime Classification
Apr 10, 2004	Apr 14, 2004	Sarasota, FL	Misdemeanor	Misdemeanor Second D
Offense Code	**Offense Description**	**Grade of Offense**	**Degree of Offense**	**Case Type**
322.03(4)	Operate Motorcycle Without Lic	SECOND DEGREE MISDEMEANOR	Second Degree Misdemeanor	Nc - Criminal Traffi
Case Number	**Arresting Agency**	**Court Name**	**Plea**	**Disposition**
2004CT006182NC	Sarasota Police Department	County	Nc	Adj W/h By Judge
Disposition Date	**Status**	**Count**	**Original Charge**	**Original Statute Code**
May 14, 2004	Closed	1	Operate Motorcycle W/o Lic	322.03(4)
Seq	**Ticket Number**	**Case Status Date**	**Plea Date**	**Receivedate**
1	8683dcb	05/14/2004	05/14/2004	12/31/2018
Casecomments=total Fees	**Caseinfo=uniform Case Number**	**Caseinfo**		
$152.25	582004ct006182xxxanc	Uniform Case Number: 582004ct006182xxxanc		

May 18, 2004 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Crime Classification
May 18, 2004	May 20, 2004	Florida Sarasota, FL	Traffic	Infraction
Offense Code	**Offense Description**	**Grade of Offense**	**Degree of Offense**	**Case Type**
316.187(2)(A)	Unlawful Speed 70mph Zone	N/A MOVING INFRACTION	N/a Moving Infraction	North County Traffic
Case Number	**Arresting Agency**	**Court Name**	**Plea**	**Disposition**
2004TR022601NC	Florida Highway Patrol	County	Guilty	Pd Civil Penalty - Traffic Infractions Only
Disposition Date	**Status**	**Casecomments=total Fees**	**Caseinfo=uniform Case Number**	**Count**
Jun 21, 2004	Closed	$155.00	582004tr022601xxxanc	1
Original Charge	**Original Statute Code**	**Seq**	**Ticket Number**	**Case Status Date**
Unlawful Speed 70mph Zone	316.187(2)(a)	1	7049crf	06/21/2004
Plea Date	**Receivedate**	**Caseinfo**		
06/21/2004	12/31/2018	Uniform Case Number: 582004tr022601xxxanc		

Feb 20, 2004 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Crime Classification
Feb 20, 2004	Feb 20, 2004	Florida Sarasota, FL	Traffic	Infraction
Offense Code	**Offense Description**	**Grade of Offense**	**Degree of Offense**	**Case Type**
316.183(2)	Unlawful Speed	N/A MOVING INFRACTION	N/a Moving Infraction	South County Traffic
Case Number	**Arresting Agency**	**Court Name**	**Plea**	**Disposition**
2004TR008178SC	North Port Police Department	County	Guilty	Pd Civil Penalty - Traffic Infractions Only
Disposition Date	**Status**	**Casecomments=total Fees**	**Caseinfo=uniform Case Number**	**Count**
May 12, 2004	Closed	$184.00	582004tr008178xxxasc	1
Original Charge	**Original Statute Code**	**Seq**	**Ticket Number**	**Case Status Date**
Unlawful Speed	316.183(2)	1	7371cgp	05/12/2004
Plea Date	**Receivedate**	**Caseinfo**		
05/12/2004	12/31/2018	Uniform Case Number: 582004tr008178xxxasc		

Mar 1, 2004 - Charges Filed - Unlawful Speed 70mph Zone

Charges Filed Date	Crime Classification	Offense Code	Offense Description	Grade of Offense
Mar 1, 2004	Itv	316.187(2)(A)	Unlawful Speed 70mph Zone	INFRACTION

Case Number	Court Name	Disposition	Disposition Date	Status
2004TR009628NC	County	Pd Civil Penalty - Traffic Infractions Only	May 26, 2004	Closed

Caseinfo

Uniform Case Number: 582004tr009628xxxanc

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Offense Date	Source
Jul 13, 2004	SARASOTA COUNTY CIRCUIT COURT (Florida)

Personal Details

First Name	Last Name	Age	Date of Birth	Address
Jason	Williams	46	Mar 11, 1974	86023 W 26th St # 114, Bradenton, Manatee

Jul 13, 2004 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Offense Code
Jul 13, 2004	Jul 14, 2004	Sarasota, FL	Misdemeanor	784.03(1A1)
Offense Description	**Grade of Offense**	**Degree of Offense**	**Case Type**	**Case Number**
Battery Domestic	FIRST DEGREE MISDE-MEANOR	First Degree Misde-meanor	Sc - Misdemeanor	2004MM011253SC
Disposition Date	**Status**	**Count**	**Obts Number**	**Original Charge**
Sep 3, 2004	Closed	1	5802015948	Battery Domestic
Original Statute Code	**Prosecutor Final Action**	**Seq**	**Case Status Date**	**Receivedate**
784.03(1a1)	Da	1	09/03/2004	12/31/2018

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Offense Date	Source
Feb 26, 2004	SARASOTA COUNTY CIRCUIT COURT (Florida)

Personal Details

First Name	Last Name	Age	Date of Birth	Address
Jason	Williams	46	Mar 11, 1974	6713 Myrtlewood Rd, North Port, Sarasota

Feb 26, 2004 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Offense Code
Feb 26, 2004	Mar 1, 2004	Sarasota, FL	Traffic	316.187(2)(A)

Offense Description	Grade of Offense	Degree of Offense	Case Type	Case Number
Unlawful Speed 70mph Zone	N/A MOVING INFRAC-TION	N/a Moving Infraction	North County Traffic	2004TR009628NC
Arresting Agency	**Plea**	**Disposition Date**	**Status**	**Count**
Sarasota County Sher-iff'S Office	Guilty	Mar 1, 2004	Closed	1
Original Charge	**Original Statute Code**	**Seq**	**Ticket Number**	**Case Status Date**
Unlawful Speed 70mph Zone	316.187(2)(a)	1	6042dgx	05/26/2004
Plea Date	**Receivedate**			
05/26/2004	12/31/2018			

Jason A Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Charges Filed Date	Source
Jan 10, 1996	MARTIN COUNTY MUNICIPAL COURT (Florida)

Personal Details

First Name	Middle Initial	Last Name	Age	Date of Birth
Jason	A	Williams	46	Mar 11, 1974

Physical Appearance

Ethnicity	Height
White	5'10"

Jan 10, 1996 - Charges Filed - Fail To Renew Mtr Veh Reg Exp More 4 Mos

Charges Filed Date	Crime Location	Offense Code	Offense Description	Case Number
Jan 10, 1996	Martin, FL	FAIL TO RENEW MTR VEH REG EXP MORE 4 MOS	Failure To Renew Mtr Ve-hicle Reg Exp More 4 Mos	96000302MMAXMX
Disposition	**Disposition Date**	**Status**	**Case Id Number**	**Charge Count Number**
Bond Estreature	Jan 9, 1996	Closed	158380	001
Receivedate				
02/03/2020				

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Offense Date	Source
Jun 10, 2004	MANATEE CIRCUIT AND COUNTY COURT (Florida)

Personal Details

First Name	Last Name	Age	Date of Birth	Address
Jason	Williams	46	Mar 11, 1974	86023 W 26th St # 114, Bradenton, Manatee

Physical Appearance

Ethnicity
Black

Jun 10, 2004 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Offense Code
Jun 10, 2004	Jun 11, 2004	Manatee, FL	Traffic	316.189(1)
Offense Description	**Case Type**	**Case Number**	**Arresting Agency**	**Plea**
Unlawful Speed In A Municipality	Traffic Infractions	2004TR019039AX	Bpd	Nolo-Contendere
Status	**Count**	**Ticket Number**	**Receivedate**	
Collections-Open	1	6490con	03/27/2018	

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Offense Date	Source
Jun 8, 2007	MANATEE CIRCUIT AND COUNTY COURT (Florida)

Personal Details

First Name	Last Name	Age	Date of Birth	Address
Jason	Williams	46	Mar 11, 1974	321 9th Street Dr W, Palmetto, Manatee

Physical Appearance

Ethnicity	Height	Weight
Black	5'0"	140 lbs

Jun 8, 2007 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Crime Classification
Jun 8, 2007	Jun 11, 2007	Manatee, FL	Felony	Felony
Offense Code	**Offense Description**	**Degree of Offense**	**Case Type**	**Case Number**
893.135(1B1A)	Armed Trafficking In Cocaine With A Firearm (28 Gr	First Degree Life	Felony	2007CF002299AX
Arresting Agency	**Arrest Date**	**Disposition**	**Disposition Date**	**Status**
Mso	Jun 8, 2007	Dropped/abandoned	Jun 26, 2007	Closed
Count	**Receivedate**			
1	03/27/2018			

Jun 8, 2007 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Crime Classification
Jun 8, 2007	Jun 11, 2007	Manatee, FL	Felony	Felony
Offense Code	**Offense Description**	**Degree of Offense**	**Case Type**	**Case Number**
812.019(1)	Dealing In Stolen Property (second Degree)	Second Degree	Felony	2007CF002299AX
Arresting Agency	**Arrest Date**	**Disposition**	**Disposition Date**	**Status**
Mso	Jun 8, 2007	Dropped/abandoned	Jun 26, 2007	Closed
Count	**Receivedate**			
2	03/27/2018			

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Offense Date	Source
Feb 11, 2003	ADMINISTRATIVE OFFICE OF COURTS (Connecticut)

Personal Details

First Name	Last Name	Age	Date of Birth	Address
Jason	Williams	46	Mar 11, 1974	78 Third Ave, Seymour, New Haven

Feb 11, 2003 - Offense -

Offense Date	Crime Classification	Offense Code	Offense Description	Grade of Offense
Feb 11, 2003	Infraction	14-99G(G)	Ill Opn Mv Wo Tint In-spection	INFRACTION
Counts	**Case Number**	**Arresting Agency**	**Arrest Date**	**Court Name**
1	MI033476202S	State Police Troop 'I'	Feb 11, 2003	A05d - Ansonia At Derby
Court Costs	**Plea**	**Disposition Date**	**Caseinfo=new Plea**	**Caseinfo**
$50.00	Ng	Apr 17, 2003	Gy; Init Plea Wthdrw Date: 20030417	New Plea: Gy; Init Plea Wthdrw Date: 20030417

Jason A Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Source

DEPT OF CORRECTIONS (-Florida)

Personal Details

First Name	Middle Initial	Last Name	Age	Date of Birth
Jason	A	Williams	46	Mar 11, 1974

Physical Appearance

Ethnicity

White

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Charges Filed Date	Source
Apr 14, 2004	SARASOTA COUNTY CIRCUIT COURT (Florida)

Personal Details

First Name Last Name Age Date of Birth

Jason	Williams	46	Mar 11, 1974

Apr 14, 2004 - Charges Filed - Operate Motorcycle W/O Lic

Charges Filed Date	Crime Location	Offense Code	Offense Description	Case Number
Apr 14, 2004	Sarasota, FL	322.03(4)	Operate Motorcycle Without Lic	582004-CT0061820001NC

Court Name	Disposition	Disposition Date
Fl Sarasota County Circuit Court	Adj W/h By Judge	May 14, 2004

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Charges Filed Date	Source
Jul 14, 2004	SARASOTA COUNTY CIRCUIT COURT (Florida)

Personal Details

First Name	Last Name	Age	Date of Birth
Jason	Williams	46	Mar 11, 1974

Jul 14, 2004 - Charges Filed - Battery-Touch Or Strike

Charges Filed Date	Crime Location	Offense Code	Offense Description	Case Number
Jul 14, 2004	Sarasota, FL	784.03(1A1)	Battery-touch Or Strike	582004-MM0112530001SC

Court Name	Disposition	Disposition Date
Fl Sarasota County Circuit Court	Dropped/abandoned	Sep 3, 2004

Jason Anthony Williams

Match Rating Based On:

First Name, Middle Name, Last Name, Date Of Birth, Address, Age

Charges Filed Date	Source
May 22, 1992	ADMINISTRATIVE OFFICE OF COURTS (North Carolina)

Personal Details

First Name	Middle Name	Last Name	Age	Date of Birth
Jason	Anthony	Williams	46	Mar 11, 1974

Address

4110 Sedgewood Dr Apt 305, Raleigh, Wake

Physical Appearance

Ethnicity

White

May 22, 1992 - Charges Filed - Unspecified

Charges Filed Date	Crime Location	Offense Code	Offense Description	Case Type

May 22, 1992	Wake, Wake, NC	UNSPECIFIED	Unspecified	Criminal
Case Number	Case Sequence	Case Year	Disposed	Last Update Date
01910-WAKE1992CR01291 9	012919	1992	Y	07/04/2020

Jason Williams

Match Rating Based On:

First Name, Last Name, Date Of Birth, Age

Offense Date	Source
Jun 8, 2007	FLORIDA_MANATEE_COUNTY (Florida)

Personal Details

First Name	Last Name	Age	Date of Birth
Jason	Williams	46	Mar 11, 1974

Physical Appearance

Complexion

Black

Jun 8, 2007 - Offense -

Offense Date	Charges Filed Date	Crime Classification	Offense Code	Offense Description
Jun 8, 2007	Jun 11, 2007	F	893.135 1B1A	Armed Trafficking In Cocaine With A Firearm (28 Gr
Grade of Offense	**Degree of Offense**	**Case Type**	**Case Number**	**Disposition**
FELONY	First Degree, Life	Felony	412007CF002299AX	Dropped/abandoned
Disposition Date	**Status**	**Caseinfo**		
Jun 26, 2007	Closed	Sao Case Number: 2007 Sa 011137, Otbs Number: 4103116402		

Jun 8, 2007 - Offense -

Offense Date	Charges Filed Date	Crime Classification	Offense Code	Offense Description
Jun 8, 2007	Jun 11, 2007	F	812.019 1	Dealing In Stolen Property (second Degree)
Grade of Offense	**Degree of Offense**	**Case Type**	**Case Number**	**Disposition**
FELONY	Second Degree	Felony	412007CF002299AX	Dropped/abandoned
Disposition Date	**Status**	**Caseinfo**		
Jun 26, 2007	Closed	Sao Case Number: 2007 Sa 011137, Otbs Number: 4103116402		

Less Likely Criminal Records

Jason Williams

Match Rating Based On:

First Name, Last Name

Charges Filed Date Source

Jul 18, 1990

ADMINISTRATIVE OFFICE OF COURTS (North Carolina)

Personal Details

First Name	Last Name	Address
Jason	Williams	4110 Sedgewood Dr Apt 305, Raleigh, Wake

Jul 18, 1990 - Charges Filed - Not Specified

Charges Filed Date	Crime Location	Offense Code	Offense Description	Case Type
Jul 18, 1990	Wake, NC	NOT SPECIFIED	Not Specified	Criminal

Case Number	Court Name
9101990CR051895	Wake

Jason Williams

Match Rating Based On:

First Name, Last Name

Charges Filed Date	Source
Oct 9, 1995	ADMINISTRATIVE OFFICE OF COURTS (North Carolina)

Personal Details

First Name	Last Name	Address
Jason	Williams	Rr 10 Box 308 # A14, Fayetteville, Cumberland

Physical Appearance

Ethnicity

Black

Oct 9, 1995 - Charges Filed - Not Specified

Charges Filed Date	Crime Location	Offense Code	Offense Description	Case Type
Oct 9, 1995	Cumberland, NC	NOT SPECIFIED	Not Specified	Criminal

Case Number	Court Name
2501995CR046745	Cumberland

Jason Williams

Match Rating Based On:

First Name, Last Name

Offense Date	Source
Jun 18, 1990	ADMINISTRATIVE OFFICE OF COURTS (North Carolina)

Personal Details

First Name	Last Name	Address
Jason	Williams	4110 305 Sedgewood D # R, Raleigh, Wake

Jun 18, 1990 - Offense -

Offense Date	Charges Filed Date	Crime Location	Crime Type	Offense Code
Jun 18, 1990	Jul 17, 1990	Wake, NC	Misdemeanor	49-2
Offense Description	**Case Type**	**Case Number**	**Court Name**	**Disposition**
Arraigned:non Iv-d Non-supp Illegit Child	Misdemeanor	01910WAKE1990CR-051895	Wake	Dismissal Without Leave By Da
Disposition Date				
Jun 7, 1991				

Sex Offender Information

This section displays the names, locations, and offenses of individuals charged with sex crimes living in close proximity to the locations associated with the subject of this report. Individuals listed below may have been charged with sex crimes as indicated. We make no representation as to the current status of these individuals. Some individuals listed below may no longer be required to register or report to state sex offender registries.

Nearby

5016 Wynneford Way, Raleigh, NC 27614-9810

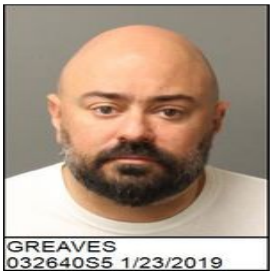
Lionel Quinto, 30

Location Details

7726 Sandra Ln, Raleigh, NC 27615-5015

Charge/Offense

Sexual battery.



Jamie Scott Greaves, 44

Location Details

1613 River Mill Dr, Wake Forest, NC 27587-9521

Charge/Offense

Indecent liberty minor.

Jerome Curtis Bohringer, 61

Location Details

Last Reported Address - Out Of State, Raleigh, NC 27615

Charge/Offense

Sex offense other state (sexual exploitation of a minor (third degree) (2 counts)).

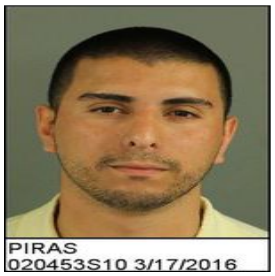
Tommy Horton, 39

Location Details

808 Ivanhoe Dr, Raleigh, NC 27615-2216

Charge/Offense

Registered as a result of out-of-state conviction.



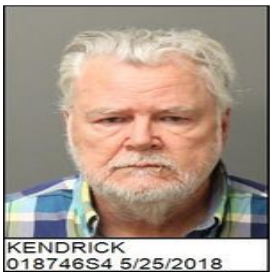
Frank Ricardo Piras, 29

Location Details

400 Lynchester Ct, Raleigh, NC 27615-7301

Charge/Offense

Indecent liberty minor.



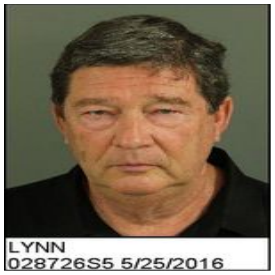
Jackie Kendrick, 73

Location Details

9003 Grassington Way, Raleigh, NC 27615-9106

Charge/Offense

Registered as a result of out-of-state conviction.



Thomas Jefferson Lynn, 69

Location Details
1301 Durlain Dr, Raleigh, NC 27614-6424

Charge/Offense
Sexual battery.

Matthew Jon Gibson, 30

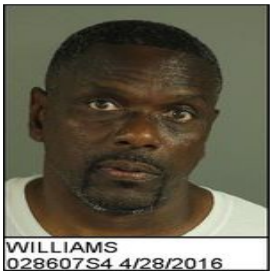
Location Details
2224 Valley Edge Dr, Raleigh, NC 27614-7362

Charge/Offense
Sex exploit minor 2nd degree.

Sean Forrest Aitken, 43

Location Details
8413 Astwell Ct, Raleigh, NC 27615-8124

Charge/Offense
Sexual battery.



Ronnie Lewis Williams, 60

Location Details
10632 Dehijuston Ct, Raleigh, NC 27614-8765

Charge/Offense
Attempted rape or attempted sex offense (1st,2nd degree).

Clarence Michael Allen, 51

Location Details
7012 Longstreet Dr, Raleigh, NC 27615-6323

Charge/Offense
Sexual battery.

Eric Anthony Copeland, 26

Location Details
10724 Cokesbury Ln, Raleigh, NC 27614-6716

Charge/Offense
Sexual battery.

Jackie Kendrick, 73

Location Details
Last Reported Address - Out Of State, Raleigh, NC 27614

Charge/Offense
Lewd or lascivious molestation victim under 12 years offender 18 or older; f.s. 800.04(5)(b) (principal).

Markel Devon Braxton, 43

Location Details
2225 Raven Rd, Raleigh, NC 27614-6772

Charge/Offense
Attempted rape or attempted sex offense (1st,2nd degree).

Blake Lee Spencer-, 51

Location Details
Last Reported Address - Out Of State, Raleigh, NC 27615

Charge/Offense
Sex offense other state (indecent liberties with child).

Benjamin Barrett Talbott, 37

Location Details
9206 Grassington Way, Raleigh, NC 27615-9101

Charge/Offense
Registered as a result of out-of-state conviction.

Ronald Virgil Clifton, 55

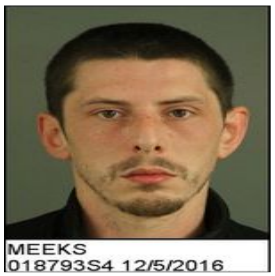
Location Details
7812 Haymarket Ln, Raleigh, NC 27615-5441

Charge/Offense
Registered as a result of out-of-state conviction.

Larry Princeton Guins, 74

Location Details
7913 Wood Cove Ct, Raleigh, NC 27615-4732

Offense Code
NC034439S2



James Wesley Meeks, 33

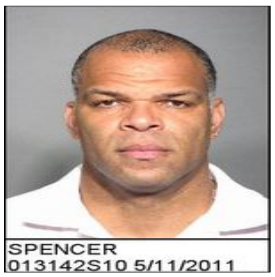
Location Details
8812 Litchford Rd, Raleigh, NC 27615-2420

Charge/Offense
Sexual battery.

John Sanders, 52

Location Details
Last Reported Address - Out Of State, Raleigh, NC 27615

Charge/Offense
Sex bat/ wpn. or force; f.s. 794.011(3) (principal in attempt).



John Anthony Spencer, 54

Location Details
11308 Stoney Woods Dr, Raleigh, NC 27614-7598

Offense Code
NC013142S10

Edward Dwayne Collins, 57

Location Details
12124 Lock Lockhart Ln, Raleigh, NC 27614

Charge/Offense
Sodomy with a minor under 16 years of age and offender is over 21 years of age.

Jerome Curtis Bohringer, 61

Location Details

6401 New Market Way, Raleigh, NC 27615-6823

Charge/Offense

Sex exploit minor 3rd degree.

Jeremy Samuel Jones, 33

Location Details

120 Farrington Dr, Raleigh, NC 27615-2974

Charge/Offense

Indecent liberty minor.

Jerome Curtis Bohringer, 61

Location Details

6401 New Market Way, Raleigh, NC 27615-6823

Charge/Offense

Child pornography/film/photos (6 counts).

Social Profiles

This section contains possible online profiles and articles for the subject of this report.

LinkedIn

Jason Williams

https://www.linkedin.com/in/jason-a-williams-35a620a0

Current Job:

Partner at Morgan Creek Blockchain Capital

Previous Jobs:

Partner at Morgan Creek Digital Assets

Co Founder and General Partner at Morgan Creek Digital Assets

Angel Investor at Duke Angel Network

Angel Investor at RTP Capital Associates, Inc.

Managing Partner at Full Tilt Capital

Member Board of Trustess at Louisburg College

Angel Investor at Undercover Colors

Advisor to Innovations in Healthcare at Duke University School of Medicine

Angel Investor at Fortnight Brewing

Angel Investor at FishBetter

President and CEO at PRTI Inc

Healthcare Catalyst and Team Builder at Angel investor - Social Entrepreneur

Angel Investor at Penda Health

Angel Investor / President / Board Member at PRTI Inc

Member of the Board of Directors at PRTI Inc

President at PRTI

Innovations in Healthcare at Duke University

Angel Investor at JuiceVibes

Angel Investor at Dermasensa Laboratories

Angel Investor at 13C Molecular

Member Board of Trustees at Methodist University

Angel Investor at Pierros Italian Bistro

Founder and Former President and CEO, President and CEO of the Eastern Region at FastMed

Founder at FastMed

Orthopedic Surgical Physician Assistant at Cape Fear Orthopedics

Emergency Physician Assistant at PhyAmerica

Education:

Doctor of Humanities, honoris causa from Methodist University

Master's Degree, Master of Physician Assistant Studies from University Of Nebraska-lincoln

Surgical training, Advanced Training in General Surgery from Yale University School Of Medicine

Bachelor of Health Science (BHS), Physician Assistant from Methodist University

Bachelor of Science (B.S.), Human Biology from Methodist University

Addresses:

Fayetteville, North Carolina

Henderson, Nevada

Clayton, North Carolina, 27520

Florida

Louisburg, North Carolina, 27549

Raleigh, North Carolina

Cary, North Carolina

Durham, North Carolina

Related URLs

http://www.fastmed.com
http://www.prtitech.com
https://www.linkedin.com/...
https://www.linkedin.com/...
https://www.linkedin.com/...

User's ID

a0/620/35a@linkedin

359853046@linkedin

#35a620a0@linkedin

Industry

Renewables & Environment

Volunteering

Board Of Trustees At Methodist University

Medical Aid At African Mission Work

Skills

Medicine

Leadership

Entrepreneurship

Strategic Planning

Marketing Strategy

Healthcare Management

Customer Service

Business Strategy

Healthcare Information

Medical Coding

EMR

Clinical Research

Medical Billing

Surgery

Operations Management

Private Equity Funding

Branding & Identity

Talent Management

Talent Acquisition

Medical Practice

Conflict Management

Growth Strategies

Acquisitions

Land Development

Interior Design

Corporate Development

Medical Practice Operations

Medical Practice Management

Organic Chemistry

Start-ups

Healthcare Information Technology (HIT)

Electronic Medical Record (EMR)

Title

President And CEO PRTI; Active Investor

Co-Founder, Morgan Creek Digital Assets, CEO PRTI

Groups

Anesthesia Coding Updates

Society Of Physician Entrepreneurs (SoPE)

Urgent Care Association Of America

Global Physician Assistant Professionals

Medical Coders And Billers

Local Connection Lab

AAPI Health Network-For Doctors Physicians Nurses Hospitals Clinics IT Healthcare Service Providers

PA (Physician Assistant) Professional Network

Africa: The New Frontier For Angel Investors, Venture Capitalists And Startups

Manchester United Football Club Group

Global Healthcare Investment And Investors, M&A Professionals

UCAOA Group Discussion Page

Global Healthcare Resources & Investment & Investors | Healthcare Innovation And Disruption

UCA Group Discussion Page

Connections

500+ Connections

Global Healthcare Resources &-
Investment & Investors | Healthcare
Innovation And Disruption

Facebook

Jason Williams

jason.a.williams.79

Usernames:	Facebook Friends	User's ID
jason.a.williams.79	Jasyn Rymer	1591719689@facebook

NPPES NPI Registry

Jason Williams

https://npiregistry.cms.hhs.gov/registry/provider-view/1932432481

Current Job:	Addresses:
OWNER at BOONE UC INC	11373 Us Highway 70 W, Clayton, North Carolina, 27520

USA Business Contact

Jason Williams

Current Job:	Addresses:
at WILLIAMS, JASON A	2001 S Main Street, Wake Forest, North Carolina, 27587

fastmed.com

https://www.fastmed.com/about-fastmed/news-and-press/fastmed-urgent-care-launches-keep-cooler-program/

Addresses:	Title	Preview
North Carolina	FastMed Urgent Care Launches Keep Cooler Program	Jason Williams, MPAS, Ph.D Or Reuel Heyden 919-550-0821 X1016 J.williams@fastmed.com

USA Business

Jason Williams

Current Job:	Addresses:
at WILLIAMS, JASON A	2001 S Main Street, Wake Forest, North Carolina, 27587

Business Emails

Jason Williams

Current Job:
at louisburg college

Residential Address

Jason Williams

Addresses:
5016 Wynneford Way, Raleigh, North Carolina, 27614

1010 Clarendon Street, Fayetteville, North Carolina, 28305

3212 Se Aster Lane, Stuart, Florida, 34994

901 Tallstone Drive, Fayetteville, North Carolina, 28311

2713 Preston Woods Lane, Fayetteville, North Carolina, 28304

Professional license

Jason Williams

Current Job:	Addresses:
Physician Assistant	2001 S Main Street, Wake Forest, North Carolina, 27587

Domain owner WW

Jason Williams

Current Job:	Addresses:	Associated Domain
at ExSme	5016 Wynneford Way, Raleigh, North Carolina, 27614	Prtitech.net
		Therapybridge.org

Auto owners US

Jason Williams

Addresses:	Auto Make	Auto Model	Auto Vin
5016 Wynneford Way, Raleigh, North Carolina, 27614	Mercedes-Benz	S-Class	WDDNG7DB6DA499267
	Mercedes-Benz	S-Class	WDDNG71X89A246085
		E-Class	WDBUF56X77B009907
		G-Class	WDCYC3HF1AX183190

Address history reco

Jason Williams

Addresses:
5016 Wynneford Way, Raleigh, North Carolina, 27614

1010 Clarendon Street, Fayetteville, North Carolina, 28305

1805 James Street, Durham, North Carolina, 27707

2911 Banner Street, Durham,
North Carolina, 27704

2314 B Lednum Avenue, Durham,
North Carolina, 27704

1203 Gilbert Street, Durham,
North Carolina, 27701

2314 Ledum Street, Durham,
North Carolina, 27705

2314 Lednum Street, Durham,
North Carolina, 27705

1114 N Driver Street, Durham,
North Carolina, 27701

2314 A Lednum Avenue, Durham,
North Carolina, 27704

Email owners USA

Jason Williams

Addresses:

5016 Wynneford Way, Raleigh,
North Carolina, 27614

Domain owners US

Jason Williams

Current Job:

at ExSme

Addresses:

5016 Wynneford Way, Raleigh,
North Carolina, 27614

Residential Contacts

Jason Williams

Addresses:

5016 Wynneford Way, Raleigh,
North Carolina, 27614

NPPES NPI Registry

Jason Williams

https://npiregistry.cms.hhs.gov/registry/provider-view/1609949288

Addresses:

1010 Clarendon Street, Fayet-
teville, North Carolina, 28305

Business Profiles

This section includes business related information that we have found on this person such as business affiliations or employment history.

Possible Business Affiliations

Examination Of What LLC

DUNS Number	061497027	Primary Company Names	Examination Of What LLC
Current Address	5016 Wynneford Way, Raleigh, NC 27614-9810		

Lakeview Urgent Care

DUNS Number	130406288	Primary Company Names	Lakeview Urgent Care
Current Address	3622 N Main St, Hope Mills, NC 28348-1937		

Layman & Williams Holdings Inc

DUNS Number	092918807	Primary Company Names	Layman & Williams Holdings Inc Layman And Williams Holdings, Inc.
Current Address	3950 Fairsted Dr Apt 705, Raleigh, NC 27612-4591		

Tienta Transport Inc

DUNS Number	117481553	Primary Company Names	Tienta Transport Inc
Current Address	528 S 4th St, Smithfield, NC 27577-4474	Former Address	Po Box 1923, Smithfield, NC 27577-1923

Urgent Care Family Clinics Of America, Inc.

DUNS Number	088133226	Primary Company Names	Williams And Perkins Holdings Williams And Perkins Holdings, LLC
Current Address	5016 Wynneford Way, Raleigh, NC 27614-9810		

Williams And Lorenzo Property Management, LLC

DUNS Number	080711130	Primary Company Names	Williams And Lorenzo Property Management, LLC Williams Lrnzo Prperty Mgt LLC
Current Address	5016 Wynneford Way, Raleigh, NC 27614-9810		

Williams Management Systems In

DUNS Number	176752603	Primary Company Names	Williams Management Systems In Williams Management Systems, Inc.
Current Address	1010 Clarendon St, Fayetteville, NC 28305-4847		

Corporate Filings

100% Compliance, Inc. (Primary)

Business Name	100% COMPLIANCE, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	935 Shotwell Rd, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Multi Status
Filing Number	#1082920	Verification Date	Dec 7, 2019
Filing Office DUNS Number	#361860265	Received Date	Dec 10, 2019
Filing Date	Feb 6, 2009	File Date	Dec 12, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	935 Shotwell Rd, Clayton, NC 27520-5597

100% Compliance, Inc. (Primary)

Business Name	100% COMPLIANCE, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	935 Shotwell Rd, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Multi Status
Filing Number	#1082920 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Feb 6, 2009	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	935 Shotwell Rd, Clayton, NC 27520-5597

Asheville Urgent Care, P.C. (Primary)

Business Name	ASHEVILLE URGENT CARE, P.C.		
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1077556 -PA	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Dec 31, 2008	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Asheville Urgent Care, P.C. (Primary)

Business Name	ASHEVILLE URGENT CARE, P.C.		
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1077556	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Dec 31, 2008	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Boone Uc, Inc. (Primary)

Business Name	BOONE UC, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#1114328	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Sep 4, 2009	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Boone Uc, Inc. (Primary)

Business Name	BOONE UC, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#1114328 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Sep 4, 2009	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Cedar Creek Medical Group, P.A. (Primary)

Business Name	CEDAR CREEK MEDICAL GROUP, P.A.	Incorporation State	NC
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	4101 Macon Pond Rd # 215, Raleigh, NC 27607		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0655054 -PA	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Dec 5, 2002	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	935 Shotwell Rd Ste 108, Clayton, NC 27520-5598

Cedar Creek Medical Group, P.A. (Primary)

Business Name	CEDAR CREEK MEDICAL GROUP, P.A.	Incorporation State	NC
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	4101 Macon Pond Rd # 215, Raleigh, NC 27607		
Address Type	Mailing	Registration Type	Corporation
State	NC		Dissolved

		Securities And Exchange Commission Status	
Filing Number	#0655054	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Dec 5, 2002	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	935 Shotwell Rd Ste 108, Clayton, NC 27520-5598

Comprehensive Virtual Healthcare, Inc. (Primary)

Business Name	COMPREHENSIVE VIRTUAL HEALTHCARE, INC.		
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Administrative Dissolution
Filing Number	#1445564 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	May 14, 2015	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Comprehensive Virtual Healthcare, Inc. (Primary)

Business Name	COMPREHENSIVE VIRTUAL HEALTHCARE, INC.		
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Administrative Dissolution
Filing Number	#1445564	Verification Date	Oct 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Oct 15, 2019
Filing Date	May 14, 2015	File Date	Oct 21, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Cpjw, Inc. (Primary)

Business Name	CPJW, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	

			300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Multi Status
Filing Number	#1074508 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Dec 8, 2008	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Cpjw, Inc. (Primary)

Business Name	CPJW, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Multi Status
Filing Number	#1074508	Verification Date	Oct 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Oct 15, 2019
Filing Date	Dec 8, 2008	File Date	Oct 21, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Fuquay Urgent Care & Family Clinic, Inc. (Former)

Business Name	FUQUAY URGENT CARE & FAMILY CLINIC, INC.	Incorporation State	NC
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0672571 -PA	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Apr 23, 2003	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Fuquay Urgent Care & Family Clinic, Inc. (Former)

Business Name	FUQUAY URGENT CARE & FAMILY CLINIC, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Converted
Filing Number	#0672571 -BUS	Verification Date	Jan 22, 2016
Filing Office DUNS Number	#361860265	Received Date	Jan 27, 2016
Filing Date	Apr 23, 2003	File Date	Feb 2, 2016
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Fuquay Urgent Care & Family Clinic, Inc. (Former)

Business Name	FUQUAY URGENT CARE & FAMILY CLINIC, INC.	Incorporation State	NC
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0672571	Verification Date	May 31, 2019
Filing Office DUNS Number	#361860265	Received Date	Jun 4, 2019
Filing Date	Apr 23, 2003	File Date	Jun 15, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Guha, Perkins And Williams, Llc (Primary)

Business Name	GUHA, PERKINS AND WILLIAMS, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address			

	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0623960	Verification Date	Oct 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Oct 15, 2019
Filing Date	Mar 14, 2002	File Date	Oct 21, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Guha, Perkins And Williams, Llc (Primary)

Business Name	GUHA, PERKINS AND WILLIAMS, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0623960 -LLC	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Mar 14, 2002	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Hendersonville Urgent Care, P.C. (Primary)

Business Name	HENDERSONVILLE URGENT CARE, P.C.		
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1097381	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	May 14, 2009	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Hendersonville Urgent Care, P.C. (Primary)

Business Name	HENDERSONVILLE URGENT CARE, P.C.		
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1097381 -PA	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	May 14, 2009	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Juicevibes, Llc (Primary)

Business Name	JUICEVIBES, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11692 Us 70 Business Hwy W # Bus, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Active
Filing Number	#1380281 -LLC	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	May 20, 2014	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Juicevibes, Llc (Primary)

Business Name	JUICEVIBES, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11692 Us 70 Business Hwy W # Bus, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Active
Filing Number	#1380281	Verification Date	Jan 8, 2021
Filing Office DUNS Number	#361860265	Received Date	Jan 11, 2021
Filing Date	May 20, 2014	File Date	Jan 15, 2021
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Mill Lake, L.L.C. (Primary)

Business Name	MILL LAKE, L.L.C.	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	5016 Wynneford Way, Raleigh, NC 27614		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Active
Filing Number	#0778192	Verification Date	Oct 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Oct 15, 2019
Filing Date	Apr 20, 2005	File Date	Oct 21, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Tienta Transport, Inc. (Primary)

Business Name	TIENTA TRANSPORT, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	Po Box 1923, Smithfield, NC 27577		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Active
Filing Number	#1571864 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Feb 7, 2017	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Tienta Transport, Inc. (Primary)

Business Name	TIENTA TRANSPORT, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	Po Box 1923, Smithfield, NC 27577		
Address Type	Mailing	Registration Type	Corporation

State	NC	Securities And Exchange Commission Status	Active
Filing Number	#1571864	Verification Date	Mar 27, 2020
Filing Office DUNS Number	#361860265	Received Date	Mar 31, 2020
Filing Date	Feb 7, 2017	File Date	Apr 7, 2020
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Uca Pharma, Inc. (Primary)

Business Name	UCA PHARMA, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Multi Status
Filing Number	#1137191 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Feb 19, 2010	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Uca Pharma, Inc. (Primary)

Business Name	UCA PHARMA, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Multi Status
Filing Number	#1137191	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Feb 19, 2010	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Urgent Care Family Clinics Of America, Inc. (Former)

Business Name	URGENT CARE FAMILY CLINICS OF AMERICA, INC.	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	5016 Wynneford Way, Raleigh, NC 27614		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Administrative Dissolution
Filing Number	#0627985	Verification Date	Oct 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Oct 15, 2019
Filing Date	Dec 31, 2015	File Date	Oct 21, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Urgent Care Family Clinics Of America, Inc. (Former)

Business Name	URGENT CARE FAMILY CLINICS OF AMERICA, INC.	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	5016 Wynneford Way, Raleigh, NC 27614		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Active
Filing Number	#0627985 -LLC	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Dec 31, 2015	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Urgent Care Family Clinics Of America, Inc. (Former)

Business Name	URGENT CARE FAMILY CLINICS OF AMERICA, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	5016 Wynneford Way, Raleigh, NC 27614		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Converted
Filing Number	#0627985 -BUS	Verification Date	Oct 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Oct 15, 2019
Filing Date	Apr 17, 2002	File Date	Oct 21, 2019
Filing Office Name			

	Secretary Of State/Corporations Division

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Urgent Care Of Boone, P.C. (Primary)

Business Name	URGENT CARE OF BOONE, P.C.		
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1119201 -PA	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Oct 12, 2009	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Urgent Care Of Boone, P.C. (Primary)

Business Name	URGENT CARE OF BOONE, P.C.		
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1119201	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Oct 12, 2009	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Wake Urgent Care And Family Clinic, Inc. (Primary)

Business Name	WAKE URGENT CARE AND FAMILY CLINIC, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	Po Box 1306, Clayton, NC 27528		
Address Type	Mailing	Registration Type	Corporation
State	NC		Converted

		Securities And Exchange Commission Status	
Filing Number	#C673503 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Apr 30, 2003	File Date	Apr 26, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Wake Urgent Care And Family Clinic, Inc. (Primary)

Business Name	WAKE URGENT CARE AND FAMILY CLINIC, INC.	Incorporation State	NC
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	Po Box 1306, Clayton, NC 27528		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0673503 -PA	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Apr 30, 2003	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Wake Urgent Care And Family Clinic, Inc. (Primary)

Business Name	WAKE URGENT CARE AND FAMILY CLINIC, INC.	Incorporation State	NC
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	Po Box 1306, Clayton, NC 27528		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Converted
Filing Number	#C673503	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Apr 30, 2003	File Date	Apr 26, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Wake Urgent Care And Family Clinic, Inc. (Primary)

Business Name	WAKE URGENT CARE AND FAMILY CLINIC, INC.	Incorporation State	NC
Corporation Type	Professional	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	Po Box 1306, Clayton, NC 27528		
Address Type	Mailing	Registration Type	Corporation
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0673503	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Apr 30, 2003	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Williams & Ferguson, Llc (Primary)

Business Name	WILLIAMS & FERGUSON, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304		
Address Type	Business	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0599140 -LLC	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Jul 27, 2001	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304-3660

Williams & Ferguson, Llc (Primary)

Business Name	WILLIAMS & FERGUSON, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304		
Address Type	Business	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Dissolved
Filing Number	#0599140	Verification Date	May 3, 2019
Filing Office DUNS Number	#361860265	Received Date	May 7, 2019
Filing Date	Jul 27, 2001	File Date	May 9, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304-3660

Williams And Perkins, Llc (Primary)

Business Name	WILLIAMS AND PERKINS, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	5016 Wynneford Way, Raleigh, NC 27614		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Active
Filing Number	#0774815	Verification Date	Jan 24, 2020
Filing Office DUNS Number	#361860265	Received Date	Jan 28, 2020
Filing Date	Mar 31, 2005	File Date	Jan 31, 2020
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	5016 Wynneford Way, Raleigh, NC 27614-9810

Williams Management Systems, Inc. (Primary)

Business Name	WILLIAMS MANAGEMENT SYSTEMS, INC.		
Corporation Type	Profit	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Corporation
		Securities And Exchange Commission Status	Dissolved
Filing Number	#0752315 -BUS	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Nov 15, 2004	File Date	Apr 27, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	1010 Clarendon St, Fayetteville, NC 28305-4847

Williams, Perkins And Guha, Llc (Primary)

Business Name	WILLIAMS, PERKINS AND GUHA, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC		Administrative Dissolution

		Securities And Exchange Commission Status	
Filing Number	#1033119 -LLC	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Mar 17, 2008	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Williams, Perkins And Guha, Llc (Primary)

Business Name	WILLIAMS, PERKINS AND GUHA, LLC	Incorporation State	NC
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
Address	11373 Us Highway 70 W, Clayton, NC 27520		
Address Type	Mailing	Registration Type	Limited Liability Company
State	NC	Securities And Exchange Commission Status	Administrative Dissolution
Filing Number	#1033119	Verification Date	May 3, 2019
Filing Office DUNS Number	#361860265	Received Date	May 7, 2019
Filing Date	Mar 17, 2008	File Date	May 9, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Wilson Urgent Care, Pllc (Primary)

Business Name	WILSON URGENT CARE, PLLC		
Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Professional Limited Liability Company
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1047323	Verification Date	Apr 19, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 24, 2019
Filing Date	Jun 4, 2008	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Wilson Urgent Care, Pllc (Primary)

Business Name	WILSON URGENT CARE, PLLC

Corporation Type	Corporation	Filing Office Address	300 N Salisbury St # Off, Raleigh, NC 27603
Standard Industrial Classification Code	00000000		
		Registration Type	Professional Limited Liability Company
		Securities And Exchange Commission Status	Dissolved
Filing Number	#1047323 -PLLC	Verification Date	Apr 12, 2019
Filing Office DUNS Number	#361860265	Received Date	Apr 16, 2019
Filing Date	Jun 4, 2008	File Date	Apr 30, 2019
Filing Office Name	Secretary Of State/Corporations Division		

Business Contact - Jason Williams

Title	Registered Agent	Address	11373 Us Highway 70 W, Clayton, NC 27520

Employment History

Williams And Lorenzo Property Management, LLC

Employment Dates	Sep 16, 2020 - Sep 16, 2020	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Williams And Lorenzo Property Management LLC

Employment Dates	Sep 15, 2020 - Sep 15, 2020	Employer's Address	2004 S Miami Blvd, Durham, NC 27703

Examination Of What, LLC

Employment Dates	Sep 17, 2016 - Oct 22, 2019	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Mill Lake LLC

Employment Dates	Oct 7, 2019 - Oct 7, 2019	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Juicevibes Cary LLC

Employment Dates	Sep 5, 2018 - Sep 5, 2018	Employer's Address	2105 Us 1 Hwy, Franklinton, NC 27525

Williams & Ferguson LLC

Employment Dates	Jan 3, 2018 - Jan 3, 2018	Employer's Address	2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304

Juicevibes LLC

Employment Dates	Sep 17, 2016 - Oct 5, 2017	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Prti Inc

Employment Dates	Dec 13, 2016 - Jun 26, 2017	Employer's Address	4140 Parklake Ave Ste 200, Raleigh, NC 27612

Freshvibes LLC

Employment Dates	Jun 26, 2017 - Jun 26, 2017	Employer's Address	401 W 1st St, Greenville, NC 27834

Tienta Transport Inc

Employment Dates	Mar 14, 2017 - Mar 14, 2017	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Williams And Perkins Holdings LLC

Employment Dates	Sep 17, 2016 - Mar 14, 2017	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Layman And Williams Holdings Inc

Employment Dates	Feb 7, 2017 - Feb 7, 2017	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Asheville Urgent Care Pc

Employment Dates	Sep 17, 2016 - Sep 17, 2016	Employer's Address	11373 Us Highway 70 W, Clayton, NC 27520

Boone Uc Inc

Employment Dates	Sep 17, 2016 - Sep 17, 2016	Employer's Address	11373 Us Highway 70 W, Clayton, NC 27520

Cpjw Inc

Employment Dates	Sep 17, 2016 - Sep 17, 2016	Employer's Address	11373 Us Highway 70 W, Clayton, NC 27520

Hendersonville Urgent Care Pc

Employment Dates	Sep 17, 2016 - Sep 17, 2016	Employer's Address	11373 Us Highway 70 W, Clayton, NC 27520

Uca Pharma Inc

Employment Dates	Sep 17, 2016 - Sep 17, 2016	Employer's Address	

11373 Us Highway 70 W, Clayton, NC 27520

Urgent Care Of Boone Pc

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 11373 Us Highway 70 W, Clayton, NC 27520

Wake Urgent Care And Family Clinic Inc

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 11373 Us Highway 70 W, Clayton, NC 27520

Wilson Urgent Care Pllc

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 11373 Us Highway 70 W, Clayton, NC 27520

Comprehensive Virtual Healthcare Inc

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 5016 Wynneford Way, Raleigh, NC 27614

Wucfa LLC

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 4101 Lake Boone Trl, Raleigh, NC 27607

Medical Cleaning And Maintenance LLC

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 4514 Tarkiln Pl, Wake Forest, NC 27587

Guha Perkins And Williams LLC

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 11373 Us Highway 70 W, Clayton, NC 27520

Pierro S Express LLC

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 113 Person St, Fayetteville, NC 28301

Fuquay Urgent Care & Family Clinic Pc

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address: 11373 Us Highway 70 W, Clayton, NC 27520

100% Compliance Inc

Employment Dates: Sep 17, 2016 - Sep 17, 2016
Employer's Address:

			635 Shotwell Rd, Clayton, NC 27520

Williams Management Systems Inc

Employment Dates	Sep 17, 2016 - Sep 17, 2016	Employer's Address	1010 Clarendon St, Fayetteville, NC 28305

Williams And Perkins LLC

Employment Dates	Sep 17, 2016 - Sep 17, 2016	Employer's Address	5016 Wynneford Way, Raleigh, NC 27614

Lakeview Urgent Care And Family

Employment Dates	Jan 1, 2010 - Aug 1, 2016	Employer's Address	3622 N Main St, Hope Mills, NC 28348

Lakeview Urgent Care

		Employer's Address	3622 N Main St, Hope Mills, NC 28348

Licenses

Possible data may include FAA pilot licenses and DEA licenses for prescribing controlled pharmaceuticals.

Our extensive public records search did not uncover licenses information for Jason Anthony Williams.

There are 618,660 FAA certified pilots in the U.S. That's less than 0.2% of the population.
So, if FAA license information doesn't show up here, Jason Anthony Williams may not have one.

Finances

This section includes financial information that we have found on this person such as bankruptcies, liens, judgments, foreclosures or evictions.

Possible Judgments

Judgment

Name	Jason Williams	Filing Type	CIVIL JUDGMENT RELEASE
Address	1010 Clarendon St, Fayetteville, NC 28305	Filing Date	Feb 8, 2008
		Court Case Number	2008CVD000133
		Total Judgment Amount	$5457.00

Possible UCC Filings

UCC Filing

Filing Type	Original	Filing Date	Oct 7, 2020
Filing Number	20200154191G	Debtors	DANA WILLIAMS BARBOUR Address: 528 S 4th St, Smithfield, NC 27577 Born Mar 29, 1968 (Age 52) TIENTA TRANSPORT INC Address: 528 S 4th St, Smithfield, NC 27577 JASON ANTHONY WILLIAMS Address: 5016 Wynneford Way, Raleigh, NC 27614 Born Mar 11, 1974 (Age 46)
Filing Office	SECRETARY OF STATE/UCC DIVISION	Filing Office Address	300 N Salisbury St, Legis Off Bldg, Raleigh, NC 27603
		Secured Parties	THREAD CAPITAL, INC. 4021 Carya Dr, Raleigh, NC 27610

UCC Filing

Filing Type	Continuation	Filing Date	Jul 22, 2011
Filing Number	20110063454H	Debtors	ROBERT L FERGUSON Address: 6651 Burgenfield Dr, Fayetteville, NC 28314 JASON A WILLIAMS Address: 2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304 Born Mar 11, 1974 (Age 46)
Filing Office	SECRETARY OF STATE/UCC DIVISION	Filing Office Address	300 N Salisbury St, Legis Off Bldg, Raleigh, NC 27603

		Secured Parties	BRANCH BANKING AND TRUST COMPANY 3817 Morganton Rd, Fayetteville, NC 28314

UCC Filing

Filing Type	Continuation	Filing Date	Jun 16, 2006
Filing Number	20060059344E	Debtors	ROBERT L FERGUSON Address: 6651 Burgenfield Dr, Fayetteville, NC 28314 Born Jul 29, 1942 (Age 78) JASON A WILLIAMS Address: 2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304 Born Mar 11, 1974 (Age 46)
Filing Office	SECRETARY OF STATE/UCC DIVISION	Filing Office Address	300 N Salisbury St, Legis Off Bldg, Raleigh, NC 27603
		Secured Parties	BRANCH BANKING AND TRUST COMPANY 3817 Morganton Rd, Fayetteville, NC 28314

UCC Filing

Filing Type	Original	Filing Date	Sep 21, 2001
Filing Number	20010525102C	Debtors	ROBERT L FERGUSON Address: 6651 Burgenfield Dr, Fayetteville, NC 28314 Born Jul 29, 1942 (Age 78) JASON A WILLIAMS Address: 2713 Preston Woods Ln Apt 7, Fayetteville, NC 28304 Born Mar 11, 1974 (Age 46)
Filing Office	SECRETARY OF STATE/UCC DIVISION	Filing Office Address	300 N Salisbury St, Legis Off Bldg, Raleigh, NC 27603
		Secured Parties	BRANCH BANKING AND TRUST COMPANY 3817 Morganton Rd, Fayetteville, NC 28314

Assets

This section includes assets information that we have found on this person. Possible data may include properties owned, watercrafts owned and vehicles owned or driven.

Currently Owned Properties

Currently Owned Property #1

Rowan Beach Estates

24235 N Holiday Blvd
Rodanthe, North Carolina, 27968

2 beds | 1 baths | 960 sq/ft

Current Owner
Terese M Lorenzo
Jason A Williams
Sep 8, 2017

Assessed Value	Sale Amount	Tax Amount
$172,700.00	$750,000.00	$1,183.87
2020	Aug 18, 2017	2019

Property Details

Bedrooms	Bathrooms	Living Sq. Ft	Land Sq. Ft
2	1	960	10000
Floors	**Year Built**	**APN#**	**Type**
1	1978	012671000	Single Family Residence

Property Value

Land Value	Improvement Value	Assessed Value (2020)	Tax Amount (2019)
$101,300.00	$71,400.00	$172,700.00	$1,183.87

Assessed Value
2007 - 2020

2007	2009	2011	2012	2013
$352,200.00	$352,200.00	$352,200.00	$352,200.00	$168,000.00
2014	**2015**	**2016**	**2017**	**2018**
$168,000.00	$168,000.00	$168,000.00	$168,000.00	$168,000.00
2019	**2020**			
$168,000.00	$172,700.00			

Ownership History

Current Owner
Terese M Lorenzo
Jason A Williams
Sep 8, 2017

Ownership Details

Document Number	700043441	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Aug 18, 2017
Recording Date	Sep 8, 2017	Residential Model Indicator	Property is Residential
Sale Amount	$750,000.00	Title Company	ATTORNEY ONLY
Owner	Terese M Lorenzo Jason A Williams Po Box 212, Rodanthe, North Carolina, 27968	Seller	Patricia L Phillips

Previous Owner

Patricia Phillips

Sep 15, 2016

Ownership Details

Document Number	700030052	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Townhouse	Sale Date	Sep 2, 2016
Resale New Construction	Resale	Recording Date	Sep 15, 2016
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Resale, Residential (Modeled)
Title Company	ATTORNEY ONLY	Owner	Patricia Phillips 717 Donaghe St, Staunton, Virginia, 24401
Seller	M Trust Chappell Leta Patricia L Phillips		

Deed Information

Document Type	Deed	Registry Entry Date	Sep 15, 2016
Document Number	000700030052	Transaction Type	Nominal
Batch ID	20161021	Batch Sequence	00253

Deed Information

Document Type	Deed	Registry Entry Date	Aug 9, 2017
Document Number	000700042381	Transaction Type	Nominal
Batch ID	20170907	Batch Sequence	00315

Previous Owner

Allen Holland

Aug 9, 2016

Ownership Details

Document Number	700028790	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Townhouse	Sale Date	Aug 8, 2016
Resale New Construction	Resale	Recording Date	Aug 9, 2016
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Interfamily Transfer, Resale, Residential (Modeled)
Title Company	ATTORNEY ONLY	Owner	Allen Holland 1503 Ketch Ln, Kill Devil Hills, North Carolina, 27948
Seller	Rebecca G Holland		

Deed Information

Document Type	Deed	Registry Entry Date	Aug 9, 2016
Document Number	000700028790	Transaction Type	Nominal
Batch ID	20161020	Batch Sequence	00632

Previous Owner

Patricia Lee Phillips

Leta M Chappell

Aug 24, 1987

Ownership Details

Universal Land Use	Single Family Residence	Property Indicator	Single Family Residence
Resale New Construction	Resale	Recording Date	Aug 24, 1987
Absentee Indicator	Absentee(Mail And Situs Not =)	Residential Model Indicator	Property is Residential
Deed Securities Category	Resale, Residential (Modeled)	Owner	Patricia Lee Phillips Leta M Chappell 717 Donaghe St, Staunton, Virginia, 24401
Seller	Record Owner		

Deed Information

Document Type	Deed	Registry Entry Date	Aug 24, 1987
Transaction Type	Resale	Batch ID	19300101
Batch Sequence	11919		

Previous Owner

Patricia Lee Phillips

Aug 24, 1987

Ownership Details

Universal Land Use	Single Family Residence	Property Indicator	Single Family Residence
Recording Date	Aug 24, 1987	Absentee Indicator	Absentee(Mail And Situs Not =)
Residential Model Indicator	Property is Residential	Owner	Patricia Lee Phillips 717 Donaghe St, Staunton, Virginia, 24401
Seller	Record Owner		

Previously Owned Properties

Previously Owned Property #1

Devon Sub Ph 1

5016 Wynneford Way
Raleigh, North Carolina, 27614

3 baths | 7620 sq/ft

Current Owner

Jason Williams

Jennifer H Williams

Oct 17, 2012

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$985,498.00	$350,000.00	$1,400,000.00	$11,277.64
2020	Apr 2, 2012	Oct 16, 2012	2019

Property Details

Bathrooms	Living Sq. Ft	Land Sq. Ft	Floors
3	7620	56628	2

Year Built	APN#	Type

2003	1718.01-27-7712000	Single Family Residence/Town-house

Property Value

Land Value	Improvement Value	Assessed Value (2020)	Tax Amount (2019)
$290,000.00	$695,498.00	$985,498.00	$11,277.64

Assessed Value

2008 - 2020

2008	2010	2011	2012	2013
$1,106,801.00	$1,106,801.00	$1,106,801.00	$1,131,146.00	$1,184,233.00
2014	2016	2018	2019	2020
$1,184,233.00	$1,378,430.00	$1,378,430.00	$1,378,430.00	$985,498.00

Ownership History

Current Owner

Jason A Williams

Jennifer H Williams

Apr 2, 2012

Ownership Details

Universal Land Use	Single Family Residence	Property Indicator	Single Family Residence/Town-house
Sale Date	Mar 30, 2012	Resale New Construction	Resale
Recording Date	Apr 2, 2012	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Sale Amount	$1,400,000.00	Title Company	ATTORNEY ONLY
Owner	Jason A Williams Jennifer H Williams 5016 Wynneford Way, Raleigh, North Carolina, 27614	Owner Relationship Type	Husband And Wife
Seller	Call Joseph H Jr & Judi T		

Mortgage Information

Mortgage Date	Oct 16, 2012	Recording Date	Oct 17, 2012
Mortgage Amount	$1,000,000.00	Mortgage Loan Type	Conventional
Mortgage Deed Type	Deed Of Trust		

Mortgage Information

Mortgage Date	Mar 30, 2012	Recording Date	Apr 2, 2012
Mortgage Due Date	Apr 1, 2042	Mortgage Amount	$350,000.00
Mortgage Term	30 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Deed Of Trust		

Previous Owner

Joseph H Call

Judi T Call

Apr 15, 2003

Ownership Details

Universal Land Use	Vacant Land (NEC)	Property Indicator	Vacant
Sale Date	Apr 10, 2003	Recording Date	Apr 15, 2003
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Residential (Modeled)	Sale Amount	$179,000.00
Owner	Joseph H Call Judi T Call 5016 Wynneford Way, Raleigh, North Carolina, 27614	Owner Relationship Type	Husband And Wife
Seller	Young Homes Inc		

Mortgage Information

Mortgage Date	Apr 8, 2004	Recording Date	Apr 13, 2004
Mortgage Due Date	May 1, 2034	Mortgage Amount	$900,000.00
Mortgage Term	30 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Deed Of Trust		

Previous Owner

Young Homes Inc

Ownership Details

Property Indicator	Vacant	Sale Date	Apr 10, 2003
Resale New Construction	Resale	Recording Date	Apr 15, 2003
Residential Model Indicator	Based On Zip Code and Value Property is Not Residential	Deed Securities Category	Resale, Cash Purchase
Sale Amount	$179,000.00	Owner	Young Homes Inc
Seller	Creedmoor Partners LLC		

Mortgage Information

Recording Date	Apr 15, 2003	Cash Purchase	Yes

Previous Owner

Joseph Call
Judi T Call

Apr 15, 2003

Ownership Details

Property Indicator	Vacant	Sale Date	Apr 10, 2003
Resale New Construction	Resale	Recording Date	Apr 15, 2003
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)	Sale Amount	$179,000.00
Owner	Joseph Call Judi T Call 7700 Oakmont Pl, Raleigh, North Carolina, 27615	Owner Relationship Type	Husband/Wife
Seller	Young Homes Inc		

Mortgage Information

Mortgage Date	Apr 10, 2003	Recording Date	Apr 15, 2003
Mortgage Due Date	Apr 10, 2018	Mortgage Amount	$186,412.00

Mortgage Term	15 Years	Mortgage Deed Type	Deed Of Trust

Previously Owned Property #2

Highland Heights

1319 Claremont Ave
Fayetteville, North Carolina, 28305

3 beds | 2 baths | 1804 sq/ft

Current Owner
Joseph Lorenzo
Maria A Lorenzo
Jason A Williams
Jennifer Williams
Sep 1, 2015

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$150,800.00	$109,700.00	$147,000.00	$2,276.14
2019	Sep 1, 2015	Aug 25, 2015	2018

Property Details

Bedrooms	Bathrooms	Living Sq. Ft	Land Sq. Ft
3	2	1804	6098
Floors	**Year Built**	**APN#**	**Type**
1	1949	0427-96-2428	Single Family Residence/Town-house

Property Value

Land Value	Improvement Value	Assessed Value (2019)	Tax Amount (2018)
$41,250.00	$109,550.00	$150,800.00	$2,276.14

Assessed Value

2008 - 2019

2008	2009	2010	2011	2012
$115,700.00	$137,400.00	$137,400.00	$137,400.00	$137,400.00
2014	**2015**	**2016**	**2017**	**2019**
$137,400.00	$137,400.00	$137,400.00	$150,800.00	$150,800.00

Ownership History

Current Owner
Joseph Lorenzo
Maria A Lorenzo
Jason A Williams
Jennifer Williams
Sep 1, 2015

Ownership Details

Document Number	26364	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Town-house	Sale Date	Aug 25, 2015
Recording Date	Sep 1, 2015	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied

Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Title Company	STEWART TITLE GUARANTY CO	Owner	Joseph Lorenzo Maria A Lorenzo Jason A Williams Jennifer Williams 1319 Morgan Ln, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband/Wife		

Mortgage Information

Mortgage Date	Aug 25, 2015	Recording Date	Sep 1, 2015
Mortgage Due Date	Sep 1, 2035	Document Number	26364
Mortgage Amount	$109,700.00	Mortgage Term	20 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Jason A Williams
Joseph T Lorenzo

Aug 1, 2008

Ownership Details

Document Number	31675	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Jul 25, 2008
Resale New Construction	Resale	Recording Date	Aug 1, 2008
Absentee Indicator	Absentee(Mail And Situs Not =)	Residential Model Indicator	Property is Residential
Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)	Sale Amount	$147,000.00
Title Company	ATTORNEY ONLY	Owner	Jason A Williams Joseph T Lorenzo 5016 Wynneford Way, Raleigh, North Carolina, 27614
Owner Relationship Type	Married Man	Seller	Fisher Robert & Ann H

Mortgage Information

Mortgage Date	Jul 25, 2008	Recording Date	Aug 1, 2008
Mortgage Due Date	Aug 1, 2038	Document Number	31675
Mortgage Amount	$117,600.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Robert Fisher
Ann H Fisher

Dec 4, 2007

Ownership Details

Document Number	53669	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Townhouse	Sale Date	Nov 30, 2007
Resale New Construction	Resale	Recording Date	Dec 4, 2007
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)	Sale Amount	$102,000.00
Title Company	CHICAGO TITLE INSURANCE COMPAN	Owner	Robert Fisher Ann H Fisher

			716 Kooler Cir, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband/Wife	Seller	Singleton Rudolph G Iii & Sebrell C

Mortgage Information

Mortgage Date	Nov 30, 2007	Recording Date	Dec 4, 2007
Mortgage Due Date	Dec 1, 2037	Document Number	53669
Mortgage Amount	$91,800.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previously Owned Property #3

Holden Beach West

1325 Ocean Blvd W
Supply, North Carolina, 28462

6 beds | 6 baths | 3315 sq/ft

Current Owner
Thomas Weir
Sheryl B Weir
Oct 3, 2016

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$1,151,250.00	$1,046,250.00	$1,395,000.00	$6,014.81
2020	Oct 3, 2016	Sep 26, 2016	2019

Property Details

Bedrooms	Bathrooms	Living Sq. Ft	Land Sq. Ft
6	6	3315	21721
Year Built	APN#	Type	
2015	245ga036	Single Family Residence/Town-house	

Property Value

Land Value	Improvement Value	Assessed Value (2020)	Tax Amount (2019)
$525,000.00	$626,250.00	$1,151,250.00	$6,014.81

Assessed Value
2009 - 2020

2009	2010	2011	2012	2013
$1,425,000.00	$1,425,000.00	$684,000.00	$684,000.00	$684,000.00
2014	2016	2017	2018	2019
$684,000.00	$1,076,750.00	$1,076,750.00	$1,076,750.00	$1,151,250.00
2020				
$1,151,250.00				

Ownership History

Current Owner
Thomas H Weir
Sheryl B Weir
Oct 3, 2016

Ownership Details

Universal Land Use	Single Family Residence	Property Indicator	Single Family Residence/Townhouse
Sale Date	Sep 26, 2016	Resale New Construction	Resale
Recording Date	Oct 3, 2016	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)
Sale Amount	$1,395,000.00	Title Company	ATTORNEY ONLY
Owner	Thomas H Weir Sheryl B Weir 110 Bailey Cir, Kennett Square, Pennsylvania, 19348	Owner Relationship Type	Husband/Wife
Seller	Mcgee Thomas G & Kathleen M		

Mortgage Information

Mortgage Date	Sep 30, 2016	Recording Date	Oct 3, 2016
Mortgage Due Date	Nov 1, 2046	Mortgage Amount	$1,046,250.00
Mortgage Term	30 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Deed Of Trust		

Previous Owner

Thomas G McGee

Dec 29, 2014

Ownership Details

Universal Land Use	Vacant Land (NEC)	Property Indicator	Vacant
Sale Date	Dec 17, 2014	Resale New Construction	Resale
Recording Date	Dec 29, 2014	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Interfamily Transfer, Resale, Residential (Modeled)
Sale Amount	$560,000.00	Title Company	ATTORNEY ONLY
Owner	Thomas G McGee 70 Kim Ln, Long Valley, New Jersey, 07853	Seller	Kathleen A McGee Williams Jason A & Jennifer H

Mortgage Information

Mortgage Date	Feb 18, 2015	Recording Date	Feb 23, 2015
Mortgage Due Date	Feb 18, 2020	Mortgage Amount	$890,062.00
Mortgage Term	5 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Deed Of Trust		

Mortgage Information

Recording Date	Dec 29, 2014	Cash Purchase	Yes

Previous Owner

Jason A Williams

Jennifer H Williams

Jun 23, 2011

Ownership Details

Universal Land Use	Vacant Land (NEC)	Property Indicator	Vacant

Sale Date	Jun 18, 2011	Resale New Construction	Resale
Recording Date	Jun 23, 2011	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Sale Amount	$525,000.00	Title Company	ATTORNEY ONLY
Owner	Jason A Williams Jennifer H Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband And Wife
Seller	Rowena C Warren		

Mortgage Information

Mortgage Date	Oct 16, 2012	Recording Date	Oct 17, 2012
Mortgage Amount	$1,000,000.00	Mortgage Loan Type	Conventional
Mortgage Deed Type	Deed Of Trust		

Mortgage Information

Recording Date	Jun 23, 2011	Cash Purchase	Yes

Previous Owner

John D Warren

Rowena C Warren

Jan 1, 2008 - Dec 31, 2008

Ownership Details

Universal Land Use	Vacant Land (Nec)	Property Indicator	Vacant
Resale New Construction	Resale	Recording Date	Nov 1, 1989
Absentee Indicator	Absentee(Mail And Situs Not =)	Residential Model Indicator	Based On Zip Code and Value Property is Not Residential
Deed Securities Category	Resale	Owner	John D Warren Rowena C Warren 5412 Randolph Rd, Charlotte, North Carolina, 28211
Owner Relationship Type	Husband/Wife	Seller	Record Owner

Deed Information

Document Type	Deed	Registry Entry Date	Nov 1, 1989
Transaction Type	Resale	Batch ID	19300101
Batch Sequence	19825		

Previously Owned Property #4

Jason A Williams & Jennifer H

1014 Clarendon St
Fayetteville, North Carolina, 28305

3 beds | 2 baths | 2916 sq/ft

Current Owner

Hudco Investments LLC

Sep 26, 2014

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$275,500.00	$225,250.00	$265,000.00	$3,895.37
2019	Sep 26, 2014	Sep 26, 2014	2018

Property Details

Bedrooms	Bathrooms	Living Sq. Ft	Land Sq. Ft
3	2	2916	12197
Floors	**Year Built**	**APN#**	**Type**
2	1941	0437-05-6900	Single Family Residence/Town-house

Property Value

Land Value	Improvement Value	Assessed Value (2019)	Tax Amount (2018)
$68,750.00	$206,750.00	$275,500.00	$3,895.37

Assessed Value

2008 - 2019

2008	2009	2010	2011	2012
$171,200.00	$294,400.00	$294,400.00	$294,400.00	$294,400.00
2013	**2014**	**2015**	**2016**	**2017**
$294,400.00	$294,400.00	$294,400.00	$294,400.00	$275,500.00
2019				
$275,500.00				

Ownership History

Current Owner

Hudco Investments LLC

Sep 26, 2014

Ownership Details

Document Number	29090	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Town-house	Sale Date	Sep 26, 2014
Resale New Construction	Resale	Recording Date	Sep 26, 2014
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absen-tee Owner	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)	Sale Amount	$265,000.00
Title Company	ATTORNEY ONLY	Owner	Hudco Investments LLC 3603 Clinton Rd, Fayetteville, North Carolina, 28312
Seller	Williams Jason A & Jennifer H		

Mortgage Information

Mortgage Date	Sep 26, 2014	Recording Date	Sep 26, 2014
Mortgage Due Date	Sep 26, 2044	Document Number	29090
Mortgage Amount	$225,250.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Jason Williams

Jennifer H Williams

May 12, 2008

Ownership Details

Document Number	19448	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Town-house	Sale Date	Apr 25, 2008
Recording Date	May 12, 2008	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Owner	Jason Williams Jennifer H Williams 1014 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband/Wife

Mortgage Information

Mortgage Date	Apr 25, 2008	Recording Date	May 12, 2008
Mortgage Due Date	Apr 24, 2038	Document Number	19448
Mortgage Amount	$42,000.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Jason A Williams

Mar 9, 2007

Ownership Details

Document Number	10960	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Mar 6, 2007
Recording Date	Mar 9, 2007	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$296,000.00
Title Company	ATTORNEY ONLY	Owner	Jason A Williams 1014 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband And Wife	Seller	Donohoe Christian C & Jana R

Previous Owner

Jason A Williams
Jennifer H Williams

Mar 9, 2007

Ownership Details

Document Number	10960	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Mar 6, 2007
Recording Date	Mar 9, 2007	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$296,000.00
Title Company	ATTORNEY ONLY	Owner	Jason A Williams Jennifer H Williams 1014 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband And Wife	Seller	Donohoe Christian C & Jana R

Previous Owner

Jason A Williams

Mar 9, 2007

Ownership Details

Document Number	10960	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Mar 6, 2007
Recording Date	Mar 9, 2007	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$296,000.00
Title Company	ATTORNEY ONLY	Owner	Jason A Williams 1014 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband And Wife	Seller	Donohoe Christian C & Jana R

Previous Owner

Jason Williams

Jennifer H Williams

Jennifer H Williams

Mar 9, 2007

Ownership Details

Document Number	10960	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Town-house	Sale Date	Mar 6, 2007
Resale New Construction	Resale	Recording Date	Mar 9, 2007
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)	Sale Amount	$296,000.00
Title Company	ATTORNEY ONLY	Owner	Jason Williams Jennifer H Williams Jennifer H Williams 1014 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband/Wife	Seller	Donohoe Christian C & Jana R

Mortgage Information

Mortgage Date	Mar 6, 2007	Recording Date	Mar 9, 2007
Mortgage Due Date	Apr 1, 2037	Document Number	10960
Mortgage Amount	$236,800.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Jason A Williams

Jennifer H Williams

Mar 9, 2007

Ownership Details

Document Number	10960	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Mar 6, 2007
Recording Date	Mar 9, 2007	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$296,000.00
Title Company	ATTORNEY ONLY	Owner	Jason A Williams Jennifer H Williams 5016 Wynneford Way, Raleigh, North Carolina, 27614
Owner Relationship Type	Husband And Wife	Seller	Donohoe Christian C & Jana R

Previous Owner

Christian Donohoe
Jana R Donohoe
Apr 2, 2004

Ownership Details

Document Number	15624	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Town-house	Sale Date	Mar 31, 2004
Resale New Construction	Resale	Recording Date	Apr 2, 2004
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)	Sale Amount	$187,000.00
Owner	Christian Donohoe Jana R Donohoe 1014 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband/Wife
Seller	Myrtle W Vann		

Mortgage Information

Mortgage Date	Mar 31, 2004	Recording Date	Apr 2, 2004
Mortgage Due Date	Apr 1, 2034	Document Number	15624
Mortgage Amount	$193,171.00	Mortgage Term	30 Years
Mortgage Loan Type	Va(Veterans Affairs)	Mortgage Deed Type	Deed Of Trust

Previous Owner
Record Owner

Ownership Details

Universal Land Use	Single Family Residence	Property Indicator	Single Family Residence/Town-house
Resale New Construction	Resale	Recording Date	Apr 30, 2004
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Resale, Residential (Modeled)
Owner	Record Owner	Seller	Myrtle W Vann

Deed Information

Document Type	Deed	Registry Entry Date	Apr 30, 2004
Transaction Type	Nominal	Batch ID	20141108
Batch Sequence	31099		

Previously Owned Property #5

108 Gillespie St
Fayetteville, North Carolina, 28301
1 baths | 2954 sq/ft

Current Owner
Cedar Creek Crossing West LLC
Mar 24, 2014

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$225,887.00	Cash Purchase	$240,000.00	$3,231.04
2019	Mar 24, 2014	Mar 20, 2014	2018

Property Details

Bathrooms	Living Sq. Ft	Land Sq. Ft	Floors
1	2954	2178	0
Year Built	APN#	Type	
1900	0437-63-2975	Commercial	

Property Value

Land Value	Improvement Value	Assessed Value (2019)	Tax Amount (2018)
$87,246.00	$138,641.00	$225,887.00	$3,231.04

Assessed Value

2008 - 2019

2008	2009	2010	2011	2012
$55,803.00	$201,373.00	$201,373.00	$201,373.00	$201,373.00
2014	2015	2016	2017	2019
$201,373.00	$201,373.00	$201,373.00	$225,887.00	$225,887.00

Ownership History

Current Owner

Cedar Creek Crossing West LLC

Mar 24, 2014

Ownership Details

Document Number	8148	Universal Land Use	Commercial (NEC)
Property Indicator	Commercial	Sale Date	Mar 20, 2014
Resale New Construction	Resale	Recording Date	Mar 24, 2014
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner	Residential Model Indicator	Based On Zip Code and Value Property is Not Residential
Deed Securities Category	Resale, Cash Purchase	Sale Amount	$240,000.00
Title Company	ATTORNEY ONLY	Owner	Cedar Creek Crossing West LLC 23 Market Sq, Fayetteville, North Carolina, 28301
Seller	Williams Jason A & Jennifer H		

Mortgage Information

Recording Date	Mar 24, 2014	Cash Purchase	Yes
Document Number	8148		

Previous Owner

Jason Williams

Jennifer H Williams

Apr 18, 2006

Ownership Details

Document Number	17940	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Feb 9, 2006
Recording Date	Apr 18, 2006	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Not Residential	Title Company	ATTORNEY ONLY

Owner	Jason Williams Jennifer H Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband/Wife

Mortgage Information

Mortgage Date	Feb 9, 2006	Recording Date	Apr 18, 2006
Document Number	17940	Mortgage Amount	$42,000.00
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Jason Williams

Jun 3, 2005

Ownership Details

Document Number	25373	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	May 31, 2005
Recording Date	Jun 3, 2005	Absentee Indicator	Absentee(Mail And Situs Not =)
Residential Model Indicator	Property is Not Residential	Sale Amount	$134,000.00
Title Company	ATTORNEY ONLY	Owner	Jason Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband And Wife	Seller	Barbara J Sharpe

Previous Owner

Jason Williams

Jennifer Williams

Jun 3, 2005

Ownership Details

Document Number	25373	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	May 31, 2005
Recording Date	Jun 3, 2005	Absentee Indicator	Absentee(Mail And Situs Not =)
Residential Model Indicator	Property is Not Residential	Sale Amount	$134,000.00
Title Company	ATTORNEY ONLY	Owner	Jason Williams Jennifer Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband And Wife	Seller	Barbara J Sharpe

Previous Owner

Jason Williams

Jun 3, 2005

Ownership Details

Document Number	25373	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	May 31, 2005
Recording Date	Jun 3, 2005	Absentee Indicator	Absentee(Mail And Situs Not =)
Residential Model Indicator	Property is Not Residential	Sale Amount	$134,000.00
Title Company	ATTORNEY ONLY	Owner	Jason Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband And Wife	Seller	Barbara J Sharpe

Previous Owner

Jason Williams

Jennifer Williams

Jun 3, 2005

Ownership Details

Document Number	25373	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	May 31, 2005
Resale New Construction	Resale	Recording Date	Jun 3, 2005
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Not Residential
Deed Securities Category	Resale, Mortgaged Purchase	Sale Amount	$134,000.00
Title Company	ATTORNEY ONLY	Owner	Jason Williams Jennifer Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband/Wife	Seller	Barbara J Sharpe

Mortgage Information

Mortgage Date	May 31, 2005	Recording Date	Jun 3, 2005
Document Number	25373	Mortgage Amount	$84,000.00
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Barbara Sharpe

Sep 9, 2002

Ownership Details

Document Number	39610	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Sep 6, 2002
Recording Date	Sep 9, 2002	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Not Residential	Owner	Barbara Sharpe 7300 Hyannis Dr, Fayetteville, North Carolina, 28304

Mortgage Information

Mortgage Date	Sep 6, 2002	Recording Date	Sep 9, 2002
Mortgage Due Date	Sep 6, 2005	Document Number	39610
Mortgage Amount	$25,000.00	Mortgage Term	2 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previously Owned Property #6

Jason A Williams & Jennifer H

1010 Clarendon St
Fayetteville, North Carolina, 28305

4 beds | 1 baths | 3000 sq/ft

Current Owner
Mickey Hudson
Eva T Hudson
Apr 19, 2018

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$509,800.00	$200,000.00	$465,000.00	$6,937.75
2019	Apr 13, 2012	Apr 10, 2018	2018

Property Details

Bedrooms	Bathrooms	Living Sq. Ft	Land Sq. Ft
4	1	3000	23958
Floors	**Year Built**	**APN#**	**Type**
2	1920	0437-05-7902	Single Family Residence/Town-house

Property Value

Land Value	Improvement Value	Assessed Value (2019)	Tax Amount (2018)
$123,750.00	$386,050.00	$509,800.00	$6,937.75

Assessed Value

2008 - 2019

2008	2009	2010	2011	2012
$331,100.00	$479,000.00	$479,000.00	$479,000.00	$479,000.00
2014	**2015**	**2016**	**2017**	**2019**
$479,000.00	$479,000.00	$479,000.00	$509,800.00	$509,800.00

Ownership History

Current Owner
Mickey G Hudson
Eva T Hudson
Apr 13, 2012

Ownership Details

Document Number	13590	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Town-house	Sale Date	Apr 12, 2012
Resale New Construction	Resale	Recording Date	Apr 13, 2012
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Residential (Modeled)	Sale Amount	$465,000.00
Title Company	DATA SEARCH INC	Owner	Mickey G Hudson Eva T Hudson 1010 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband/Wife	Seller	Williams Jason A & Jennifer H

Mortgage Information

Mortgage Date	Apr 10, 2018	Recording Date	Apr 19, 2018
Document Number	11719	Mortgage Amount	$402,000.00
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Mortgage Information

Mortgage Date	Sep 11, 2015	Recording Date	Oct 1, 2015
Mortgage Due Date	Sep 11, 2025	Document Number	29675
Mortgage Amount	$261,300.00	Mortgage Term	10 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Mortgage Information

Mortgage Date	Apr 30, 2012	Recording Date	Jun 28, 2012
Mortgage Due Date	Apr 30, 2027	Document Number	23730
Mortgage Amount	$175,000.00	Mortgage Term	15 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Mortgage Information

Mortgage Date	Apr 12, 2012	Recording Date	Apr 13, 2012
Mortgage Due Date	May 1, 2027	Document Number	13590
Mortgage Amount	$200,000.00	Mortgage Term	15 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Mickey G Hudson

Apr 13, 2012

Ownership Details

Document Number	13590	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Apr 12, 2012
Recording Date	Apr 13, 2012	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$465,000.00
Owner	Mickey G Hudson 1010 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband And Wife
Seller	Williams Jason A & Jennifer H		

Previous Owner

Mickey G Hudson
Eva T Hudson

Apr 13, 2012

Ownership Details

Document Number	13590	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Apr 12, 2012
Recording Date	Apr 13, 2012	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$465,000.00
Owner	Mickey G Hudson Eva T Hudson 1010 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband And Wife
Seller	Williams Jason A & Jennifer H		

Previous Owner

Jason A Williams

Jan 1, 2008 - Dec 31, 2008

Ownership Details

Universal Land Use	Single Family Residence	Property Indicator	Single Family Residence
Sale Date	Oct 7, 1992	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$37,000.00
Owner	Jason A Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband And Wife
Seller	Harper Edna W & George D		

Previous Owner

Jason Williams

Jennifer H Williams

Mar 21, 2007

Ownership Details

Document Number	13047	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence/Town-house	Sale Date	Feb 27, 2007
Recording Date	Mar 21, 2007	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Title Company	TRANSUNION SETTLEMENT SOLUTION	Owner	Jason Williams Jennifer H Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband/Wife		

Mortgage Information

Mortgage Date	Feb 27, 2007	Recording Date	Mar 21, 2007
Mortgage Due Date	Feb 27, 2037	Document Number	13047
Mortgage Amount	$150,000.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Jason A Williams

Feb 28, 2003

Ownership Details

Document Number	9863	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Feb 25, 2003
Recording Date	Feb 28, 2003	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Residential	Sale Amount	$287,500.00
Owner	Jason A Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband And Wife
Seller	Harper James & Edna W		

Previous Owner

Jason A Williams
Jennifer H Williams
Feb 28, 2003

Ownership Details

Document Number	9863	Universal Land Use	Single Family Residence
Property Indicator	Single Family Residence	Sale Date	Feb 25, 2003
Resale New Construction	Resale	Recording Date	Feb 28, 2003
Absentee Indicator	Owner Occupied	Residential Model Indicator	Property is Residential
Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)	Sale Amount	$287,500.00
Owner	Jason A Williams Jennifer H Williams 1010 Clarendon St, Fayetteville, North Carolina, 28305	Owner Relationship Type	Husband And Wife
Seller	Harper James & Edna W		

Mortgage Information

Mortgage Date	Feb 26, 2003	Recording Date	Feb 28, 2003
Mortgage Due Date	Mar 1, 2033	Document Number	9863
Mortgage Amount	$287,500.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previously Owned Property #7

H C Blackwell

3622 N Main St
Hope Mills, North Carolina, 28348

5270 sq/ft

Current Owner
Mill Lake LLC
Jan 1, 2014 - Dec 31, 2014

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$318,120.00	Cash Purchase	$302,500.00	$4,812.19
2019	Apr 18, 2005	Apr 14, 2005	2018

Property Details

Living Sq. Ft	Land Sq. Ft	Year Built	APN#
5270	21780	1970	0414-55-8003

Type
Commercial

Property Value

Land Value	Improvement Value	Assessed Value (2019)	Tax Amount (2018)
$86,414.00	$231,706.00	$318,120.00	$4,812.19

Ownership History

Current Owner
Lake Llc Mill
Mill Lake LLC
Apr 18, 2005

Ownership Details

Document Number	17196	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Apr 14, 2005
Resale New Construction	Resale	Recording Date	Apr 18, 2005
Absentee Indicator	Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Not Residential
Deed Securities Category	Resale, Cash Purchase	Title Company	ATTORNEY ONLY
Owner	Lake Llc Mill Mill Lake LLC 3622 N Main St, Hope Mills, North Carolina, 28348	Seller	Jason A Williams

Mortgage Information

Recording Date	Apr 18, 2005	Cash Purchase	Yes
Document Number	17196		

Previous Owner

Robert Lee
Frances L Ferguson

Oct 29, 2001

Ownership Details

Document Number	46144	Universal Land Use	Commercial Building
Property Indicator	Single Family Residence/Townhouse	Sale Date	Oct 24, 2001
Recording Date	Oct 29, 2001	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Owner	Robert Lee Frances L Ferguson 3622 N Main St, Hope Mills, North Carolina, 28348	Owner Relationship Type	Husband/Wife

Mortgage Information

Mortgage Date	Oct 24, 2001	Recording Date	Oct 29, 2001
Mortgage Due Date	Oct 24, 2016	Document Number	46144
Mortgage Amount	$415,000.00	Mortgage Term	15 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Jason Williams
Robert L Ferguson

Aug 2, 2001

Ownership Details

Document Number	33119	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Jul 25, 2001
Resale New Construction	Resale	Recording Date	Aug 2, 2001
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner	Residential Model Indicator	Based On Zip Code and Value Property is Not Residential
Deed Securities Category	Resale, Cash Purchase	Sale Amount	$302,500.00
Title Company	ATTORNEY ONLY	Owner	

			Jason Williams Robert L Ferguson 2713 Preston Woods Ln Apt 7, Fayetteville, North Carolina, 28304
Seller	Clifton H Brock		

Mortgage Information

Recording Date	Aug 2, 2001	Cash Purchase	Yes
Document Number	33119		

Previous Owner

Mill Lake LLC

Aug 2, 2001

Ownership Details

Document Number	33119	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Jul 25, 2001
Recording Date	Aug 2, 2001	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Not Residential	Sale Amount	$302,500.00
Title Company	ATTORNEY ONLY	Owner	Mill Lake LLC 7483 Rockfish Rd, Fayetteville, North Carolina, 28306
Seller	Clifton H Brock		

Previously Owned Property #8

217 Hay St
Fayetteville, North Carolina, 28301

8646 sq/ft

Current Owner

Williams & Lorenzo Prop Mgmt L

May 27, 2009

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$792,733.00	Cash Purchase	$250,000.00	$11,230.37
2019	Dec 12, 2007	Feb 12, 2009	2018

Property Details

Living Sq. Ft	Land Sq. Ft	Year Built	APN#
8646	4356	1930	0437-54-7245

Type

Commercial

Property Value

Land Value	Improvement Value	Assessed Value (2019)	Tax Amount (2018)
$221,138.00	$571,595.00	$792,733.00	$11,230.37

Ownership History

Current Owner

Williams & Lorenzo Prop Mgmt L

Dec 12, 2007

Ownership Details

Document Number	54757	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Sep 20, 2007
Resale New Construction	Resale	Recording Date	Dec 12, 2007
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner	Residential Model Indicator	Based On Zip Code and Value Property is Not Residential
Deed Securities Category	Interfamily Transfer, Resale, Cash Purchase	Title Company	CHICAGO TITLE INSURANCE COMPAN
Owner	Williams & Lorenzo Prop Mgmt L 217 Hay St, Fayetteville, North Carolina, 28301	Seller	Jennifer Williams Jason Williams

Mortgage Information

Mortgage Date	Feb 12, 2009	Recording Date	May 27, 2009
Mortgage Due Date	Feb 12, 2024	Document Number	19445
Mortgage Amount	$227,000.00	Mortgage Term	15 Years
Mortgage Deed Type	Construction Deed Of Trust		

Mortgage Information

Mortgage Date	Aug 15, 2008	Recording Date	Aug 25, 2008
Document Number	35400	Mortgage Amount	$176,937.00
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Mortgage Information

Recording Date	Dec 12, 2007	Cash Purchase	Yes
Document Number	54757		

Previous Owner

Jason Williams
Jennie Williams
Jennifer Williams

Ownership Details

Document Number	8220	Universal Land Use	Commercial Building
Property Indicator	Single Family Residence/Townhouse	Sale Date	Feb 13, 2004
Recording Date	Feb 23, 2004	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Residential (Modeled)	Owner	Jason Williams Jennie Williams Jennifer Williams
Owner Relationship Type	Husband/Wife		

Mortgage Information

Mortgage Date	Feb 13, 2004	Recording Date	Feb 23, 2004
Mortgage Due Date	Feb 13, 2019	Document Number	8220
Mortgage Amount	$137,500.00	Mortgage Term	15 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Williams & Lorenzo Property

Jul 1, 2003

Ownership Details

Document Number	34662	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Jun 26, 2003
Recording Date	Jul 1, 2003	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Not Residential	Sale Amount	$250,000.00
Title Company	CHICAGO TITLE INSURANCE COMPAN	Owner	Williams & Lorenzo Property 217 Hay St, Fayetteville, North Carolina, 28301
Seller	Thompson Mark S & Demetrice M		

Previous Owner

Williams & Lorenzo Property Management LLC

Jul 1, 2003

Ownership Details

Document Number	34662	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Jun 26, 2003
Recording Date	Jul 1, 2003	Absentee Indicator	Owner Occupied
Residential Model Indicator	Property is Not Residential	Sale Amount	$250,000.00
Title Company	CHICAGO TITLE INSURANCE COMPAN	Owner	Williams & Lorenzo Property Management LLC 217 Hay St, Fayetteville, North Carolina, 28301
Seller	Thompson Mark S & Demetrice M		

Previous Owner

Williams & Lorenzo Prop Mgmt L

Jul 1, 2003

Ownership Details

Document Number	34662	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Jun 26, 2003
Recording Date	Jul 1, 2003	Absentee Indicator	Situs From Sale (Occupied)
Residential Model Indicator	Property is Not Residential	Sale Amount	$250,000.00
Title Company	CHICAGO TITLE INSURANCE COMPAN	Owner	Williams & Lorenzo Prop Mgmt L 217 Hay St, Fayetteville, North Carolina, 28301
Seller	Thompson Mark S & Demetrice M		

Previous Owner

Jason Williams

Jennifer Williams

Jul 1, 2003

Ownership Details

Document Number	34662	Universal Land Use	Commercial Building
Property Indicator	Commercial	Sale Date	Jun 26, 2003
Resale New Construction	Resale	Recording Date	Jul 1, 2003
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner	Residential Model Indicator	Based On Zip Code and Value Property is Not Residential
Deed Securities Category	Resale, Mortgaged Purchase	Sale Amount	$250,000.00
Title Company	CHICAGO TITLE INSURANCE COMPAN	Owner	Jason Williams Jennifer Williams

			1010 Clarendon St, Fayetteville, North Carolina, 28305
Owner Relationship Type	Husband/Wife	Seller	Thompson Mark S & Demetrice M

Mortgage Information

Mortgage Date	Jun 30, 2003	Recording Date	Jul 1, 2003
Document Number	34662	Mortgage Amount	$245,000.00
Mortgage Loan Type	Conventional	Mortgage Deed Type	Deed Of Trust

Previous Owner

Williams & Lorenzo Property Management LLC

Jul 1, 2003

Ownership Details

Document Number	34662	Universal Land Use	Commercial (Nec)
Property Indicator	Commercial	Sale Date	Jun 26, 2003
Recording Date	Jul 1, 2003	Absentee Indicator	Absentee(Mail And Situs Not =)
Residential Model Indicator	Property is Not Residential	Sale Amount	$250,000.00
Title Company	CHICAGO TITLE INSURANCE COMPAN	Owner	Williams & Lorenzo Property Management LLC 5016 Wynneford Way, Raleigh, North Carolina, 27614
Seller	Thompson Mark S & Demetrice M		

Previously Owned Property #9

Village Stuart Condo

3212 Se Aster Ln Apt Q212
Stuart, Florida, 34994

2 beds | 1200 sq/ft

Current Owner

Paula Buncy

Jul 31, 2007

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$59,207.00	$72,000.00	$80,000.00	$669.51
2020	Dec 27, 2002	Jul 13, 2007	2020

Property Details

Bedrooms	Living Sq. Ft	Year Built	APN#
2	1200	1983	38-38-41-011-016-0201.0-1-0000

Type

Condominium (Residential)

Property Value

Improvement Value	Assessed Value (2020)	Tax Amount (2020)
$99,000.00	$59,207.00	$669.51

Ownership History

Current Owner

Paula Marie Buncy

Dec 27, 2002

Ownership Details

Document Number	1623750	Universal Land Use	Condominium
Property Indicator	Condominium (Residential)	Sale Date	Dec 20, 2002
Resale New Construction	Resale	Recording Date	Dec 27, 2002
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Residential (Modeled)	Sale Amount	$80,000.00
Title Company	ATTORNEY ONLY	Owner	Paula Marie Buncy 3212 Se Aster Ln Apt Q212, Stuart, Florida, 34994
Owner Relationship Type	Single Woman	Seller	Vicki Oberle

Mortgage Information

Mortgage Date	Jul 13, 2007	Recording Date	Jul 31, 2007
Mortgage Due Date	Jul 12, 2017	Document Number	2029628
Mortgage Amount	$25,500.00	Mortgage Term	10 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Mortgage

Mortgage Information

Mortgage Date	Apr 7, 2005	Recording Date	Apr 15, 2005
Mortgage Due Date	May 1, 2035	Document Number	1830709
Mortgage Amount	$95,200.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Mortgage

Mortgage Information

Mortgage Date	Dec 20, 2002	Recording Date	Dec 27, 2002
Mortgage Due Date	Jan 1, 2033	Document Number	1623750
Mortgage Amount	$72,000.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Mortgage

Previous Owner

Jason Williams

Jan 29, 2002

Ownership Details

Document Number	1549106	Universal Land Use	Condominium
Property Indicator	Condominium (Residential)	Sale Date	Jan 7, 2002
Recording Date	Jan 29, 2002	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Owner	Jason Williams 3212 Se Aster Ln # 000203, Stuart, Florida, 34994	Owner Relationship Type	Married

Mortgage Information

Mortgage Date	Jan 7, 2002	Recording Date	Jan 29, 2002
Mortgage Due Date	Jan 7, 2017	Document Number	1549106
Mortgage Amount	$47,369.00	Mortgage Term	15 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Mortgage

Previous Owner

Vicki Tuccillo

Apr 25, 2001

Ownership Details

Universal Land Use	Condominium	Property Indicator	Condominium (Residential)
Sale Date	Apr 12, 2001	Resale New Construction	Resale
Recording Date	Apr 25, 2001	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)
Sale Amount	$30,900.00	Title Company	SOUTH FLORIDA TITLE SVCS INC
Owner	Vicki Tuccillo 3212 Se Aster Ln Apt Q212, Stuart, Florida, 34994	Owner Relationship Type	Single
Seller	Harrb B Wellman		

Mortgage Information

Mortgage Date	May 10, 2001	Recording Date	May 16, 2001
Mortgage Due Date	Jun 1, 2016	Mortgage Amount	$32,000.00
Mortgage Term	15 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Mortgage		

Mortgage Information

Recording Date	Apr 25, 2001	Cash Purchase	Yes

Previous Owner

Harry Wellman

Jan 24, 2001

Ownership Details

Universal Land Use	Condominium	Property Indicator	Condominium (Residential)
Sale Date	Jan 10, 2001	Resale New Construction	Resale
Recording Date	Jan 24, 2001	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)
Sale Amount	$56,000.00	Title Company	STEWART TITLE/MARTIN COUNTY
Owner	Harry Wellman 3922 Se Fairway W, Stuart, Florida, 34997	Owner Relationship Type	Unmarried Man
Seller	Linda J Eastman		

Mortgage Information

Mortgage Date	Jan 22, 2001	Recording Date	Jan 24, 2001
Mortgage Due Date	Jan 31, 2016	Mortgage Amount	$31,712.00
Mortgage Term	15 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Mortgage		

Previous Owner

Linda Eastman

Apr 2, 1998

Ownership Details

Universal Land Use	Condominium	Property Indicator	Condominium (Residential)
Sale Date	Mar 31, 1998	Resale New Construction	Resale
Recording Date	Apr 2, 1998	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)
Sale Amount	$50,000.00	Owner	Linda Eastman 3213 Se Aster Ln, Stuart, Florida, 34994
Owner Relationship Type	Single	Seller	Virgilio F Faticianti

Mortgage Information

Mortgage Date	Mar 31, 1998	Recording Date	Apr 2, 1998
Mortgage Due Date	Apr 1, 2028	Mortgage Amount	$45,000.00
Mortgage Term	30 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Mortgage		

Previously Owned Property #10

Village Stuart Condo

3212 Se Aster Ln Apt Q210
Stuart, Florida, 34994

2 beds | 1200 sq/ft

Current Owner

April Newswander

Oct 1, 2015

Assessed Value	Mortgage Amount	Sale Amount	Tax Amount
$50,097.00	$72,000.00	$100,000.00	$610.78
2020	Oct 27, 2003	Sep 16, 2015	2020

Property Details

Bedrooms	Living Sq. Ft	Year Built	APN#
2	1200	1983	38-38-41-011-016-0203.0-7-0000

Type

Condominium (Residential)

Property Value

Improvement Value	Assessed Value (2020)	Tax Amount (2020)
$99,000.00	$50,097.00	$610.78

Ownership History

Current Owner

April Newswander

Oct 27, 2003

Ownership Details

Document Number	1703529	Universal Land Use	Condominium
Property Indicator	Condominium (Residential)	Sale Date	Oct 16, 2003

Resale New Construction	Resale	Recording Date	Oct 27, 2003
Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Owner Occupied	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Residential (Modeled)	Sale Amount	$100,000.00
Title Company	JUPITER LAND TITLE CO	Owner	April Newswander 3212 Se Aster Ln Apt Q210, Stuart, Florida, 34994
Owner Relationship Type	Single Woman	Seller	John Markert Jean Markert

Mortgage Information

Mortgage Date	Sep 16, 2015	Recording Date	Oct 1, 2015
Mortgage Due Date	Oct 16, 2045	Document Number	2537680
Mortgage Amount	$45,000.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Equity Or Credit Line

Mortgage Information

Mortgage Date	Oct 16, 2003	Recording Date	Oct 27, 2003
Mortgage Due Date	Nov 1, 2033	Document Number	1703529
Mortgage Amount	$72,000.00	Mortgage Term	30 Years
Mortgage Loan Type	Conventional	Mortgage Deed Type	Mortgage

Previous Owner

John Markert

Jean Markert

Mar 28, 2003

Ownership Details

Document Number	1646284	Universal Land Use	Condominium
Property Indicator	Condominium (Residential)	Sale Date	Mar 25, 2003
Resale New Construction	Resale	Recording Date	Mar 28, 2003
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Resale, Cash Purchase, Residential (Modeled)
Sale Amount	$57,000.00	Owner	John Markert Jean Markert 4916 Sw Lake Grove Cir, Palm City, Florida, 34990
Owner Relationship Type	Husband/Wife	Seller	Jason A Williams

Mortgage Information

Recording Date	Mar 28, 2003	Cash Purchase	Yes
Document Number	1646284		

Previous Owner

Ownership Details

Universal Land Use	Condominium	Property Indicator	Condominium (Residential)
Sale Date	Jan 7, 2002	Recording Date	Jan 29, 2002
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Residential (Modeled)

Mortgage Information

Mortgage Date	Jan 7, 2002	Recording Date	Jan 29, 2002
Mortgage Due Date	Jan 7, 2017	Mortgage Amount	$47,369.00

Mortgage Term	15 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Mortgage		

Previous Owner

Jason Williams

Feb 15, 2000

Ownership Details

Universal Land Use	Condominium	Property Indicator	Condominium (Residential)
Sale Date	Feb 10, 2000	Resale New Construction	Resale
Recording Date	Feb 15, 2000	Absentee Indicator	Situs Address Taken From Sales Transaction - Determined Absentee Owner
Residential Model Indicator	Based On Zip Code and Value Property is Residential	Deed Securities Category	Resale, Mortgaged Purchase, Residential (Modeled)
Sale Amount	$59,000.00	Title Company	STEWART TITLE/MARTIN COUNTY
Owner	Jason Williams 901 Tallstone Dr, Fayetteville, North Carolina, 28311	Owner Relationship Type	Single Man
Seller	Ted J Leslie		

Mortgage Information

Mortgage Date	Feb 8, 2000	Recording Date	Feb 15, 2000
Mortgage Due Date	Jan 1, 2030 - Dec 31, 2030	Mortgage Amount	$47,000.00
Mortgage Term	30 Years	Mortgage Loan Type	Conventional
Mortgage Deed Type	Mortgage		

Previous Owner

Virginia M Leslie

Dec 10, 1996

Ted J Leslie

Dec 10, 1996

Ownership Details

Universal Land Use	Condominium	Property Indicator	Condominium (Residential)
Sale Date	Nov 25, 1996	Resale New Construction	Resale
Recording Date	Dec 10, 1996	Residential Model Indicator	Based On Zip Code and Value Property is Residential
Deed Securities Category	Interfamily Transfer, Resale, Residential (Modeled)	Owner	Virginia M Leslie 17685 E Kirkwood Dr, Clinton Township, Michigan, 48038Ted J Leslie 17685 E Kirkwood Dr, Clinton Township, Michigan, 48038
Seller	Virginia M Leslie Tedc J Leslie		

Deed Information

Document Type	Quit Claim	Registry Entry Date	Dec 10, 1996
Transaction Type	Nominal	Batch ID	19350102
Batch Sequence	19045		

Deed Information

Document Type	Quit Claim	Registry Entry Date	Dec 10, 1996
Transaction Type	Nominal	Batch ID	19350102

Vehicles Owned or Driven

Toyota Prius

Vehicle Identification Number (VIN)

JTDKB20UX53033613

Mercedes Benz G Class

Vehicle Identification Number (VIN)

WDCYC3HF1AX183190

Mercedes-Benz S-Class

Vehicle Identification Number (VIN)

WDDNG7DB6DA499267

Mercedes-Benz E-Class

Vehicle Identification Number (VIN)

WDBUF56X77B009907

Mercedes-Benz S-Class

Vehicle Identification Number (VIN)

WDDNG71X89A246085

Toyota Prius

Vehicle Identification Number (VIN)

JTDKB20UX53033644